警子ちゃん 4G シリーズ

DN-1500GL
LAN 対応監視･警告
プラットフォーム

取扱説明書

2014 年 09 月 26 日版
Rev.2.2

VCCI 規格適合について：

この装置は、クラス A 情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。 VCCI-A

RoHS 指令適合について：

本製品、DN-1500GL は、RoHS 指令に準拠した製品です。
This product, DN-1500GL is RoHS compliant.

目　次

改 版 履 歴

Rev.番号	年 月 日	更 新 概 要
1.0	2011/12/01	初版
1.1	2011/12/27	UI の一部改良に伴う該当記載部分の変更
1.2	2012/02/16	初期化動作を詳細に記述。および表現の統一と説明を加筆
1.3	2012/06/04	無線 LAN モジュールとアクティベーションに関する説明を加筆 SNMP トラップ監視での variable-bindings について加筆 付録を大幅に追加
1.4	2012/07/11	SNMP トラップ監視設定で指定できる OID 及び variable-bindings の OID の最大長さを 58 から 256 文字に変更 ネットワーク監視の監視間隔について加筆 イベントログのログ内容一部改良に伴う一覧差替え
1.5	2012/09/03	TCP ソケット通信の機能を追加(付録 H：イベントログの更新含む) 待機点灯の機能を追加
1.6	2012/09/20	SNMP トラップ監視の specific の入力上限値を'9999'から'2147483647'に仕様変更
1.7	2012/10/18	起動完了時に、赤と緑ランプが 3 回点滅する　説明を追加 SNMP トラップ監視設定で、generic または specific の設定変更に伴い説明を加筆
1.8	2013/01/21	SNMP トラップ　variable bindings の監視機能について説明加筆。 RSH/TCP ソケット通信/SNMP コマンドの RLY コマンドについて加筆 RSH/TCP ソケット通信「-ｔ」、「-w」オプションについて加筆 設定データのエクスポート/インポート機能追加による説明加筆。 機器連携機能追加による説明加筆。
1.9	2013/05/02	メール差込文字について説明を加筆 14.150.0G 以前のファームウェアについての注意点について説明加筆
2.0	2014/02/27	無線 LAN　環境下でのファームウェア更新　について説明追記 snmpset コマンドの記述説明を補足 電源投入後ランプが全点灯し起動しない場合の説明加筆 ネットワーク監視、SNMP トラップ監視で同一ランプに対して状態の異なるアクション設定を行った場合の説明加筆 IP　アドレス初期化手順変更による記述修正
2.1	2014/05/30	ユーザ登録とダウンロードサイトの記述修正
2.2	2014/09/26	DHCP　設定の時に割り振られた IP　を表示する設定変更に伴い説明加筆 SNMP　トラップ　variable bindings　の監視機能について説明加筆

はじめに

このたびは、警子ちゃん 4G シリーズをお買い上げいただき、誠にありがとうございます。
DN-1500GL(以下、本製品)は、IT 機器やネットワーク装置の異常時にブザー鳴動、警告灯の点灯点滅、音声ファイルの再生や電子メール等により異常発生を周囲の作業者や IT 管理者にいち早く知らせるための装置です。
ご使用の前に、本取扱説明書(以下、本書)をよくお読みの上、正しくお使いください。

免責事項について

保証規定に明記されている場合を除いて、アイエスエイは当製品の使用による直接的、間接的、例外的、偶発的、結果的な損害に対し、いかなる責任も負いません。またアイエスエイは、売上や利益の損失、機器の損失、機器の使用の損失、ソフトウェアの損失、データの損失、代用あるいは第三者によるクレーム、その他いっさいの費用について責任を負いません。

用途限定について

人の生命に関わる装置など(注)には、絶対に使用しないこと

(注)：人の生命に関わる装置などとは、以下のものをいいます。
・手術室用機器
・生命維持装置(血液透析器、新生児人工保育器、血液ポンプ、人工呼吸器など)
・有毒ガスなどの排ガス、排煙装置
・消防法、建築基準法などの各種法令により設置が義務付けられている装置
・上記に準ずる装置

ご利用前に

必ずユーザ登録をしてください。ユーザ登録されていないお客様については保証期間内であってもサポートサービスが受けられない場合があります。
ユーザ登録方法：下記いずれかより、ご登録いただけます。
■製品に同梱されている「お客様登録 FAX カード」用紙に必要事項を記入し、弊社へ FAX。
■弊社ホームページから。 URL: http://www.isa-j.co.jp/support/user/

安全にお使いいただくために

この取扱説明書では、製品を安全に正しく使用し、使用者や他の人への危害や財産への被害を未然に防止するために、必ずお守りいただくことを次のように説明しています。ご使用の前に必ずお読みください。また読み終わった後は使用者が本書をいつでも参照できるところに保管してください

表示と意味は次のとおりです。

危険	取り扱いを誤った場合に使用者が死亡または重傷を負う危険が想定される内容を示します。
警告	取り扱いを誤った場合に使用者が死亡または重傷を負う可能性が想定される内容を示します。
注意	取り扱いを誤った場合に使用者が傷害を負う危険が想定される場合および物的損害のみの発生が想定される内容を示します。

危険	お客様ご自身で分解･修理･改造は絶対に行ってはいけません。
	本体、警告灯、ブザーの隙間から水などの液体や金属などの異物を入れてはいけません。

警告	異音や異臭がした場合は使用を直ちに中止して販売店にご連絡ください。
	本体、警告灯、ブザー、AC アダプタに水がかかるような場所で使用してはいけません。
	本装置に直接水や薬品などの液体をこぼしてはいけません。
	ぬれた手で電源プラグの抜き差しを行うと感電の危険があり、してはいけません。
	本体を移設したり持ち運ぶとき、落としたり、ぶつけたりして衝撃を与えてはいけません。
	雷が鳴りだしたら AC アダプタのプラグに触れてはいけません。

注意	お客様ご自身で装置内部を触ったり、修理および改造したりしないでください。本体内の金属部分でけがしたり、回路がショートして大変危険です。絶対にカバーを外さないでください。
	AC アダプタから伸びる電源コードを傷つける･破損または加工する･無理に曲げる･引っ張る･ねじる･束ねるなどしないでください。
	コンセントから AC アダプタを抜くときは電源コードを引っ張らず必ずプラグを持って抜いてください。
	AC アダプタのプラグが緩くなったり、電源コードが傷ついたときは使用しないでください。 海抜の高い場所(PC に準じる)では使用しないでください。
	強力な磁気を持っているもののそばには置かないでください。
	調理台のそばなど油煙や湯気があたるような場所に置かないでください。
	暑い場所(45℃以上)や直射日光の当たる場所では使用しないでください。 火気に近づけないでください。
	湿気やほこりの多い場所では使用しないでください。
	移動させるときは衝撃を与えないでください。
	振動の激しいところでは使用しないでください。
	ぐらついた台の上や傾いたところなど不安定な場所へは置かないでください。
	本体の上に重いものをのせないでください。
	本体を布などでおおったり、包んだりした状態で使用しないでください。

概要

DN-1500GL(以下、本製品)は、IT 機器やネットワーク装置の異常時にブザー鳴動、警告灯の点灯点滅、音声ファイルの再生や電子メール等により異常発生を周囲の作業者や IT 管理者にいち早く知らせためのネットワーク警告灯です。警告灯は、普段異常がない場合は消灯して異常時のみ点灯させることも、待機状態(何も異常がない状態)は緑(3 灯モデル)や、緑か青か白(5 灯モデル)を点灯させることもできます。

オフィスでの使用はもちろん無人観測所、工場、流通倉庫、サーバールームやデーターセンタ内施設など離れた場所に設置された装置で発生した異常をいち早く確認できます。また WAN/LAN で接続され遠方に設置された機器の遠隔監視が可能です。無線 LAN 対応品 DN-1500GL-Axxxx、または DN-1500GL-Nxxxx に無線 LAN 追加キット(DN-1500GL-WK、オプション品)を装着すると、無線 LAN 対応(Wi-Fi 準拠)の IT 環境で利用できます。

本製品単独で IP(Internet Protocol)アドレスを持つコンピュータ装置および周辺機器、ネットワーク機器の自動チェックが可能で、装置に異常があれば自動的にブザー音や音声ファイルの再生、ランプの点灯･点滅光、そして電子メール送信で通報します。

また SNMP(Simple Network Management Protocol)トラップ受信が可能で、これらをトリガとした通報も可能です。その他にシステム運用監視で使用されているネットワーク管理ソフトウェア(一般的には「ネットワークノードマネージャ(NNM)」と言われる)と連携して SLM(Service Level Management)の向上に貢献することも可能です。

本製品の設置は管理システム側(システム監視オペレーション室内)または監視対象機器側(現場機器設置近傍)の両方あるいはどちらにでも設置できます。既存のネットワーク対応警告灯｢警子ちゃん｣との連携動作(｢警子ちゃん連携｣)も可能です。

外部装置やアプリケーションからは、rsh や TCP ソケット通信を介してコマンドを送り、表示灯や音声ファイルの再生等を直接制御可能です。

主な特長

(**NEW** : 警子ちゃん 4G シリーズからの新機能および強化機能)

キーワード	主　な　特　長
監　　視	監視用ソフトウェアやサーバは不要、OS も不問。
	最大 20 ノードと最大 40 トラップの監視が可能。
	ルータ越えの監視・通知が可能。
	ping 応答時間の検知、および応答時間に対する閾値設定が可能。**NEW**
	ウォッチドッグ·タイマ機能により自己診断を行い、異常時は自動再起動。動作環境温度の異常判定も可能。**NEW**
	多くの他社製ネットワーク管理ソフトウェアとの連携が可能。
設　　定	最大 40 個(シンプル登録)の SNMP トラップ受信をトリガとしたアクション実行が可能。**NEW**
	複数の variable-bindings 指定が可能。登録したアクションを各監視に複数設定可能。**NEW**
	異常時・異常回復時に実行するリモートシェルコマンド登録が可能。(複数台の連動、ISA製遠隔電源制御装置(RPC)※1を連動させ、OSシャットダウンも可能)
	遠隔監視によりサーバやネットワーク機器の省人運転目的で、企業内サーバールームやデーターセンタでの利用に最適。管理者負担を著しく低減し、リスク低減に貢献。
	設定は Web 設定ツールにより簡単に。オンラインヘルプも各ページ用意。**NEW**
警報 / 通知	正常時に特定のランプ(緑:3 灯モデル、緑か青か白:5 灯モデル)を点灯させ、待機状態を明示することが可能。
	警報設定において、ブザー鳴動、ランプ点灯、電子メール通知に加え、音声ファイル(最大 20 ファイル登録可)再生が可能。**NEW**
	SNMP による管理、トラップによる通知が可能。
	電子メール通知機能(PC や携帯電話/スマートフォンへの送信も対応)。
直接制御	rsh コマンドを受け取り、外部装置やアプリケーションからランプや音声ファイル再生を制御可能。
	TCP ソケット通信を介して、外部装置やアプリケーションからランプや音声ファイル再生を制御可能。**NEW**
	外部の電子メール(クライアント)ソフトの仕分け機能やコマンド実行機能を利用して、ルールに従ったランプや音声ファイル再生を制御可能。
確　　認	ログ機能により、障害解析が容易。
	セキュリティ強化。IPv4 と IPv6 フルスタック　および運用監視 SNMPv3 もサポート。**NEW**
そ の 他	ギガイーサを標準搭載し、高速網から一般速度の広範囲な通信帯域に対応。無線 LAN に対応できる、Wi-Fi 準拠の無線 LAN 搭載モデルも。**NEW**
	10Base-T/100Base-Tx/1000Base-T 自動認識·切換。**NEW**

※1 Model 7040、PDU-5000 シリーズ等豊富な遠隔電源制御装置をご用意しています。詳細は ISA までお問い合せください。

第一章 初級編 - 警子ちゃんの起動～ランプを光らせるまで -

本章では、警子ちゃんの監視機能を使って、簡単なネットワーク監視を設定し、一連の設定手順や本体動作の理解を深めます。特に警子ちゃんを初めて利用される方は、この章からの読み進めをお勧めします。
ここでは主に警子ちゃんの起動から、ランプを光らせるまでの一連の流れを説明します。
本章の概要を、下記 STEP1～4 までにまとめました。詳細は次ページ以降をご確認ください。

STEP 1 お手元に届いた警子ちゃんと同梱物をご確認ください

※開梱後、念のためすぐに欠品や損傷がないか、お確かめください。

【P.07】 各部の名称と機能
> 本説明書内でも多数出てきます。

【P.09】 本体への電源投入
> 電源が入りますか？

【P.09】 ランプ/ブザーのテスト実行
> ランプは光りますか？

操作詳細は、上記ページをご参照ください

STEP 2 さぁ、準備をはじめましょう

※お届け品以外に必要なものがあります。事前にご準備ください。

【P.10】
- PC ×1
- IP アドレス ×1
- LAN ケーブル ×1

操作詳細は、上記ページをご参照ください

STEP 3 いよいよ、警子ちゃんのセットアップに入ります

・まずは、設定ツールの起動～操作、アクション登録から。

【P.11】 設定ツールの起動、ログイン
> IP アドレス変更がカギとなります。

【P.13】 警子ちゃん 4G の基本設定
> 本体情報確認や時刻設定をします。

【P.14】 警子ちゃん 4G の監視設定
> ランプやブザーなどのアクション

操作詳細は、上記ページをご参照ください

STEP 4 最後に、テスト動作とイベントログを確認してみましょう

・STEP3 で設定したように動くかテスト動作を実行ください。

【P.19】 テスト動作
> 設定したように、動きましたか？

【P.20】 イベントログ確認
> ログ(警子ちゃんの動作履歴)を確認してみましょう。

操作詳細は、上記ページをご参照ください

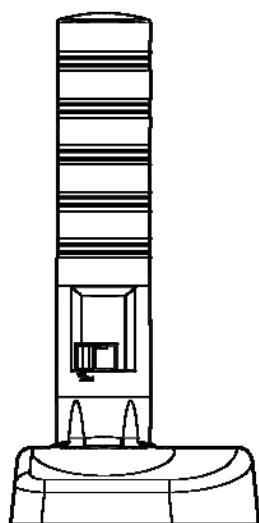
STEP 1 警子ちゃん 4G の確認

1-1 同梱品の確認

本製品には、次のものが同梱されています。すべてそろっているかご確認ください。

また輸送中に損傷を受けていないかもご確認ください。

万一欠品や損傷があった場合は(外箱の損傷についてはご容赦ください)、お買い上げの販売店までご連絡ください。

□DN-1500GL 本体 1 台

(背面の状態)

DN-1500GL-Axxxx

無線 LAN アダプタが USB ポートに装着されています

DN-1500GL-Nxxxx

無線 LAN アダプタは付属していません

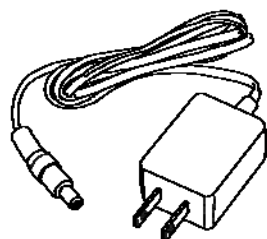
外箱の貼付ラベルで「DN-1500GL」につづく文字は各桁以下の意味があります。ご確認ください。

製品番号構成　　DN-1500GL-★●●■◆

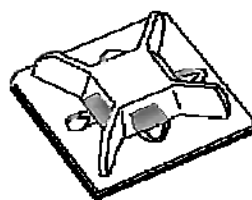
記号の意味

★	LAN タイプ	A	無線 LAN 対応
		N	無線 LAN 未対応
●●	ランプ灯数	5L	5 灯タイプ
		3L	3 灯タイプ
■	レンズ色	C	色付きレンズ
		S	透明レンズ
◆	ボディー色	B	ダークグレー
		W	ライトグレー

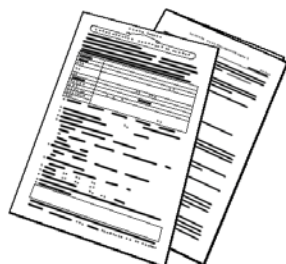
* 図は 5 灯タイプを例にした正面図および背面図です

□専用 AC アダプタ 1 個

AC100V コンセントに接続し、プラグを本体裏面の DC24V コネクタに接続して本体に電源を供給します。

*本体に電源スイッチはありません。電源投入と同時に動作します。

□マウントベース 1 個

本体裏面の空いている場所に貼り、ケーブル類の抜けを防止するための固定用台となる部品です。

*詳細は「2-1 設置する」で解説しています。

□書類 2 枚

次の 2 点です。

「お客様 FAX 登録カード兼保守契約のご案内」

「はじめにお読みください」

□結束バンド 1 本

マウントベースにケーブル類を固定する部品です。

DN-1500GL-Axxxx 無線 LAN 仕様を購入された場合、下記のものも同梱されています。

□キーシール 1 枚 Activation	アクティベーションキー記載書にあるコードをシールにし、本体底面に貼付されています。	

1-2 各部の名称と機能

本体正面／筐体部上部

図 1-1 DN-1500GL-5LCB / 5LCW /5LSB / 5LSW
(写真は DN-1500GL-5LCB)

図 1-2 DN-1500GL-3LCB / 3LCW /3LSB / 3LSW
(写真は DN-1500GL-3LCB)

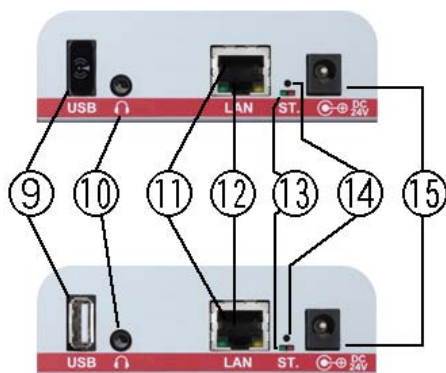
①	ランプ(赤、LED1)	⑥	ブザー音共鳴部
②	ランプ(黄、LED2)	⑦	ブザー音量調節レバー 70～90dB に調節可能
③	ランプ(青、LED6)		
④	ランプ(緑、LED3)	⑧	ALARM STOP ボタン(電源ランプを兼ねる) 3 通りの解除機能(下記参照)
⑤	ランプ(白、LED7)		

ALARM STOP ボタンによる 3 通りの解除方法：

ALARM STOP ボタンは強制的にアラームを解除する(ランプ・ブザーなどの出力を OFF にする)ためのボタンです。ALARM STOP ボタンによる解除のほかに、アラーム解除方法には 3 つのモードがあります。

強制解除	ランプの点灯、ブザー鳴動、音声ファイルの再生を強制的に止めます。 モニタ表示ページの「状態」欄に「警告」と表示されている時、または、ランプ･ブザー･音が OFF 以外の時有効です。(詳細は「アラーム解除設定」を参照)
テスト実行	長押しでランプやブザーのテストを行います。 (詳細は「ランプ･ブザーのテスト実行」を参照)
トリガアクション	ボタンを押したことをきっかけにアクションを実行します。 (詳細は「アラームストップボタンをトリガにアクション実行」を参照)

本体背面

DN-1500GL-Axxxx 背面(下図)

⑨	USB コネクタ
⑩	Audio コネクタ
⑪	LAN ポート(10/100/1000Base)
⑫	Ether リンクランプ(緑と黄 LED)
⑬	STATUS LED
⑭	RESET ボタン
⑮	電源入力コネクタ

DN-1500GL-Nxxxx 背面(上図)

図 1-3 背面

※ DN-1500GL-A(背面)写真⑨には無線 LAN アダプタがセットされています。

※ RESET ボタンを先の細い棒等で押すと本製品は再起動します。設定内容は消えません。

先の細い棒に針金等導電性の物は使わないでください。ショートの危険があります。

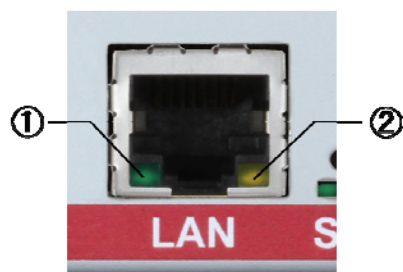
⑫ Ether リンクランプ

①	リンク状態 (緑 LED)	点灯　Link 点滅　Activity 消灯　No Link
②	接続速度 (黄 LED)	1 回点滅　10Mbps 2 回点滅　100Mbps 3 回点滅　1000Mbps

図 1-4 Ether リンクランプ

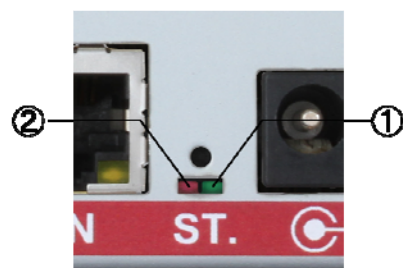
⑬ STATUS LED

①	WatchDog (緑 LED)	正常時 点滅
②	未使用	

図 1-5 STATUS LED

1-3 電源の投入 - 警子ちゃん 4G の起動

・背面の電源入力コネクタに付属の AC アダプタのプラグを接続し、AC アダプタを AC100V のコンセントに接続します。

(※本体には電源スイッチがないので、電源投入と同時にスイッチが入ります)

・電源投入から本体が起動するまで(通信できるようになるまで)1～2 分程かかります。
起動時に「赤・緑・黄」とランプが順次点灯します。その後順次消灯します。ランプ消灯が完了すると起動完了です。

本体の起動が完了するまでに、アラームストップボタンを押下すると、IP 初期化(付録 A：トラブルシューティング参照)が意図せず作動する場合があります。

・起動後、STATUS LED の右側、緑 LED(WatchDog)が点滅しているか確認します。点滅していれば正常に動作しています。

1-4 ランプ/ブザー/音声ファイル再生のテスト実行

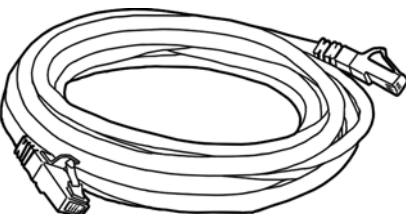
・ALARM STOP ボタンをランプが点灯するまで押し続けます。(約 5 秒)
ランプ、ブザーが順番に点灯・鳴動します。

・本製品が異常を検知している間、テストは実行されません。
警子ちゃんの web 設定ツールのトップ画面やモニタ画面（「2-7-1 監視対象の状況確認」を参照）の「状態」欄に「警告」と表示されている時、または、ランプ･ブザー･音が OFF 以外の時に有効です。

・3 灯タイプ：ランプテスト(赤→黄→緑の順で点灯)→ブザーテスト(連続、断続)。
音声ファイルの再生はランプテストと平行して行われます。

・5 灯タイプ：ランプテスト(赤→黄→緑の順で点灯)→ブザーテスト(連続、断続)→
ランプテスト(青→白の順に点灯)
音声ファイルの再生はランプテストと平行して行われます。

・ブザー音量はこのとき調整すると簡単に行えます。

※ 音声ファイルの再生を確認するには、ヘッドホン、アンプ付きスピーカ装置、PC のマイク入力等を利用します。

※ テスト用サンプル音声ファイルは、工場出荷時に登録してあります。

※ 通常状態(異常を検知していない)時、常にランプ(3 灯の場合は緑、5 灯の場合は緑・青・白から 1 色)を点灯または点滅させ、異常時は指定されたランプを消灯する「待機点灯」という機能があります。
詳細は第二章実践編の「2-5-6　待機点灯の準備」を参照ください。

STEP 2 本体設定/設置するために準備するもの

本製品の簡単な設定設置を行う際は、最低以下のものが必要になります。

PC　×1 台 ※ 以下の操作例では有線 LAN を使って行います	
IP アドレス　×1 ※ 本製品/警子ちゃんに設定するアドレスです。 ※ 例では IPv4 で設定します ※ 企業内ネットワーク環境下に設置する際、IT 管理者から事前に企業内 IP アドレスを入手しておきます	 IP アドレスとは？ インターネットやイントラネットなどの IP ネットワークに接続されたコンピュータや通信機器 1 台 1 台に割り振られた識別番号のことをいいます。
LAN ケーブル　×1 本 ※ ストレートケーブルあるいはクロスケーブルが必要となります。 ストレートの場合：本製品をハブやルータに接続して行います。 クロスの場合：PC の LAN ポートに直接接続して行います。	

STEP 3 警子ちゃん 4G のセットアップ

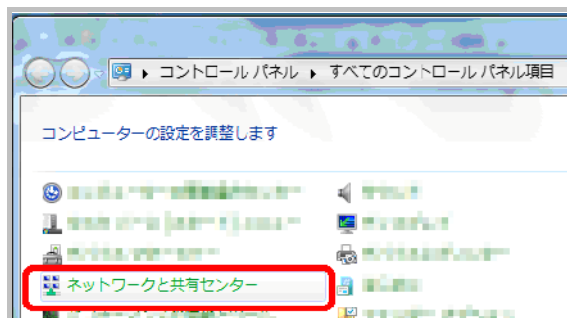
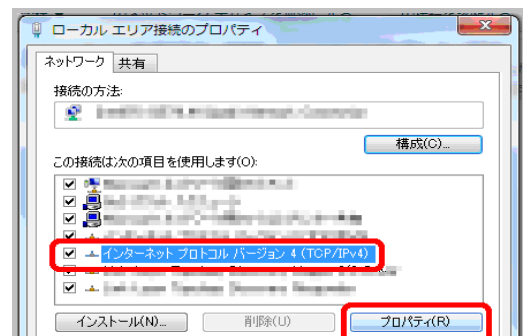
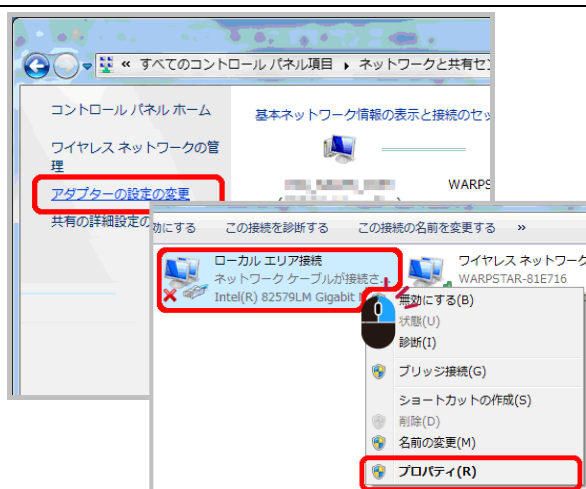
3-1 設定ツールの起動

本製品の設定変更は Web ブラウザを使って行います。ここでは、Microsoft Internet Explorer(以下 IE と略)を例に説明します(本ツールは、Microsoft IE バージョン 6 以上、Mozilla Firefox 3.6 以上で動作検証されています)。
はじめて本製品にアクセスする場合や、他のネットワークに移設し再設定する場合、次の作業が必要です。
本製品デフォルト(工場出荷時)の IP アドレスは **192.168.1.1** です。

3-1-1 使用する PC の IP アドレス変更

購入後はじめて警子ちゃん 4G 本体にアクセスする場合、本体と PC の IP アドレスを第 3 オクテットまで合わせる必要があります。ここでは設定に使用する PC の IP アドレス変更手順を説明します。
別のネットワークから警子ちゃん 4G を移設する場合は、現在本体内に登録されている IP アドレスを元に、PC の IP アドレスを決定し変更します。

Windows 7 を例に操作手順を説明します。
※ Windows 95/98/NT4.0 で設定する場合、IP アドレス変更後一旦 PC を再起動する必要があります。

<table>
<tr>
<td>①「スタート」→「コントロールパネル」→「ネットワークと共有センター」をクリック
</td>
<td>③「ローカルエリア接続のプロパティ」内の「インターネット プロトコル バージョン 4(TCP/IPv4)」を選択し「プロパティ」ボタンをクリック
</td>
</tr>
<tr>
<td>②(メニュー左側)「アダプターの設定の変更」→「ローカルエリア接続」(右クリック) →「プロパティ」をクリック</td>
<td>④「インターネット プロトコル バージョン 4 (TCP/IPv4)のプロパティが表示されます。</td>
</tr>
<tr>
<td rowspan="2">
</td>
<td>⑤プロパティ内の「IP アドレス」タブを警子ちゃん 4G と第 3 オクテットまで同じ数値にします。
ここで警子ちゃん 4G のアドレスが **192.168.1.1** なので “192.168.1” と入力し、第 4 オクテットは重複しない任意数値を入力します。
</td>
</tr>
<tr>
<td>⑥入力後「OK」をクリックし、内容を更新します。</td>
</tr>
</table>

3-1-2 本製品と PC を LAN ケーブルで接続

警子ちゃん 4G 裏面の LAN ポートと PC の LAN ポートをクロスケーブルで接続します。ハブ等のネットワーク機器を介して接続する場合はストレートケーブルで接続します
※他の機器は接続しないでください。

3-1-3 Web ブラウザから IP アドレスを入力

警子ちゃんの設定ツールは web ブラウザから利用します。Web ブラウザを開きアドレス部分に、本製品に設定されている IP アドレス(ここでは「http://**192.168.1.1**」)を入力し Enter (または Return)を押します。

3-1-4 「DN-1500GL 設定ツール」ページの表示

図 1-6 web 設定ツールトップ画面

本製品に登録されている情報と現在の状態が表示されます。
DN-1500GL 設定ツールは、IE などの Web ブラウザを使って表示や入力などを行います。従って本書では、単に「Web 設定ツール」と記述します。
トップページは機器情報と監視状況を表示していて「モニタ画面」とも記述しています。

なお図 1-6 は、サンプル画面です。日付や時間などの値は実際の表示とは異なります。

3-2 設定ツールにログイン

3-2-1 本体にログイン

図 1-7 ユーザ名とパスワードの入力画面

デフォルト(工場出荷時の)値は、以下の値です。

ユーザ名　：　DN1500
パスワード　：　DN1500

各々入力し「ログイン」ボタンをクリックします。

※「ユーザ名」と「パスワード」の変更は「管理ユーザ設定」の章で説明します。

図 1-8 設定ツールトップページ(本体情報)

ログインすると「本体情報」画面が表示されます。

3-3 警子ちゃん 4G の基本設定

3-3-1 本体情報の確認　～本製品の情報の確認～

ログイン後に表示される「本体情報」画面は、本体に登録されている「ファームウェアのバージョン」、「シリアル番号」などが表示されます。

シリアル番号の確認：

本体の底面に貼付されているシリアル番号シールの番号と本表示に相違がないかご確認ください。

万が一、相違があった場合は、販売店へご連絡ください。

ログイン後の本体情報画面	本体底面に貼られたシリアル番号シール
図 1-8 本体情報画面中のシリアル番号表示	図 1-9 本体底面のシリアル番号シール

3-3-2 日付と時刻の設定　～本製品の日付と時刻の設定をします～

手動による設定と NTP サーバを指定する設定が行えます。

日付と時間設定は、異常が発生したときのタイムスタンプとして内部で利用されます。NTP サーバがシステムに日付と時間情報を提供していれば、それと同期することで、システム全体で同一時間の事象を把握しやすくなります。

ここでは、手動による時刻設定手順を説明します。(NTP サーバの指定方法は、実践編で説明します。)

手順

1 メニュー選択

設定画面「左ナビメニュー」にある内「時刻設定」をクリックし、時刻設定画面を表示します。

2 手動による時刻設定

①「手動で設定する」にチェックし、狂いがあれば日付と時刻を入力します。

②タイムゾーンを設定します。
(例：東京、大阪、札幌：「UTC+9」)

③画面下の「設定」ボタンをクリックし、設定値に反映させます。

④設定の更新が完了すると「設定を更新しました」のメッセージが表示されます。

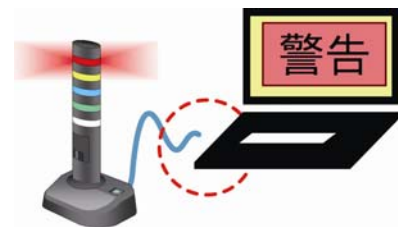
図 1-10 時刻設定画面

⑤設定画面左ナビメニュー内「モニタ表示」(「基本情報」上部分)をクリックし、「モニタ表示」画面を表示します。

⑥時刻とタイムゾーンが正しく設定されているか確認します。

図 1-11 モニタ表示(設定内容確認)

3-4 監視設定

警子ちゃん 4G では、監視対象の機器に対して一定間隔で信号を送り、一定時間内に応答があるかどうかで正常/異常を判断する、「死活監視」の機能が備わっています。
これを本解説では「ネットワーク監視」といい、最大 20 対象の機器(ノードといいます)を単独で自立して監視することができます。
他の監視方法としては、機器がネットワーク上に異常信号を送信する機能を使い、選択的にその信号を受信/判断する「トラップ監視」機能もあります。

ここでは、**警子ちゃん 4G から自分のパソコンを監視させ**、死活監視の設定方法をご紹介します。
※各項目の説明やデフォルト値は「実践編」を参照ください。

大まかな手順は、監視対象になる機器の IP アドレスを調べ、警子ちゃん 4G にそれぞれを登録し、異常を検知したとき、どのようなアクション(ランプを点滅させる、ブザーを鳴らす、音声ファイルを再生するやメールを送出するなど)を実行するか、対象ごとに設定します。
実際は対象機器の登録とアクションの設定は独立していて、監視対象とアクションとは関係づけて(紐づけて)管理することになります。

3-4-1 監視対象(ノード)の IP アドレス登録

監視対象機器の IP アドレスを調べ、警子ちゃん 4G の設定ツールを使いそれぞれを登録します。
監視対象機器の IP アドレス設定値は、管理者に聞いて入手します。

手順

1 メニュー選択

設定画面左ナビメニュー内「ネットワーク監視設定」をクリックし、「ネットワーク監視設定」画面を表示します。

2 監視対象の情報入力と登録

監視対象機器の一つを選び(ここでは警子ちゃん 4G の設定画面にアクセスしている PC)、関連情報を次の例を参考に入力していきます。
例では、「対象 01(対象機器番号 01)」を選択しています。ネットワーク監視では最大 20 の監視対象を登録できます。この登録が「対象 01」から「対象 20」に対応します。

図 1-12 ネットワーク監視設定画面

ラウンドトリップ
本製品から発信したパケットが別の監視対称機器に届き、さらにその返答が返ってくるまでの時間をいいます。

①「監視」－「有効」にチェックします。

監視対象機器に対して監視する/しないを指定します。「有効」にチェックを入れると対象機器の監視が有効になります。逆に「有効」のチェックを外すと、情報は登録されていますが、監視動作はこの機器に対して行われません。システムの検査や更新時に「有効」のチェックを外します。これにより無用のアクション実行を回避できます。
本製品では対象機器それぞれに対して独立して、「監視」する/しないを設定できます。

②「説明」には、監視対象機器が理解しやすい名称やコメントを入力します。

ここで登録された「説明」内容は、「web 設定ツールトップ画面(モニタ表示)」の「説明」欄に表示されます。
説明内容は入力してもしなくてもかまいません。「入力が任意」の項目です。
ここでは「PC 監視テスト」と入力します。

③「アドレス」には監視対象機器の IP アドレスを入力します。
入力できるアドレスは、IPv4 か IPv6 かホスト名のどれかで記述します。
例は、PC でコマンド実行画面を表示させた後、コマンドプロンプトから
ipconfig　/all 等を実行し、PC の LAN ポートに割り当てられた IP アドレス(IPv4)、
192.168.1.5 を入力した状態です。
④「監視間隔(秒)」には、監視対象機器に監視信号を送る間隔(秒)を入力します。

監視対象機器の応答特性に合わせ、個別に指定できます。一方で間隔が極端に短いとネットワークトラフィックが増加し、他の機器に影響を与える場合があります。
監視対象機器の性質やシステム設計意図などから、適切な値を入力します。
例では、1 分(60 秒)間に一度監視信号を送り出す設定です。

⑤「送信回数」は、上記④で指定された監視間隔内に送る監視信号の回数を指定します。

回数を多くすると、他のネットワーク通信に影響を与える場合があります。
例では 1 回の送出を指定しています。

⑥「平均 RTT 閾値」(RTT : Round Trip Time)では、先の④と⑤で監視対象機器に送り出された監視信号が本体に戻ってくるまでの時間をそれぞれの信号について計り、平均値を計算します。

この平均値が指定した時間(対象機器が正常に働いていてもその経路が遅くなったり、故障まででではないが反応が遅くなったりする様な場合)を閾(しきい)値として監視します。
ラウンドトリップ時間(RTT)の平均値を監視する場合は、「有効」にチェックを入れ、閾値を指定します。
　例では、PC と警子ちゃん 4G の 1 対 1 通信なので、この機能を使いません。

⑦アラートがあがった際のアクションをプルダウンの中から指定します。

ここで設定する内容は、先に設定した監視対象で異常が発生した(死活信号が帰ってこない、あるいは一定時間内に戻らない等)場合、どのアクション番号で反応し通知するかを紐付けます。
今回は「アクション 1」を選択します。アクションの内容登録は次項にて説明します。

3 設定内容の反映
画面下の「設定」ボタンをクリックし、設定値に反映させます。(設定ボタンを押すまでは、本体に記録されません。)

3-4-2 アクションの設定　～ランプ・ブザー・音声の設定～

「アクションの設定」とは、本体の監視機能で異常を検知したときどのような反応を実行するかを決め、管理者や要員に伝えるかを設計することです。伝達方法は、人に直接訴えかける光･ブザー音･音声再生･電子メール送出と、他の管理機器や装置にメッセージを送り管理システム全体で対応する方法に大別できます。

ここでは、本体周辺にいる人に直接異常を伝達する前者の機能を試してみます。

手順

1 メニュー選択

設定画面左メニューにある｢ネットワーク監視アクション一覧/設定｣をクリックし、｢ネットワーク監視アクション一覧/設定｣画面を表示します。
20 件分のアクションが一覧で確認できます。
登録件数 20 件は少ないように感じられるかもしれませんが、アクションが必要とする状況は緊急対応を必要とする場合が多く、その対応項目とアクションとを関連づける方が意味や伝達方法を決定しやすくなります。
たとえば例では PC が異常になったらアクションを実行するように進めていますが、実際の運用ではこういうアクションが実行されたらどう行動するかという関連づけが重要です。

2 アクション登録

では実際にアクションを登録してみましょう。

図 1-13 ネットワーク監視アクション一覧/設定

①登録したいアクション名をクリックし、アクションの登録画面へ移動します。

前項の監視対象の IP アドレス登録で異常を検知したら｢アクション 1｣を実行するように設定していますので、｢アクション一覧｣の中から｢アクション 1｣を選択します。すると画面が変わり、アクションを構成する機能を定義する｢アクション設定｣画面が現れます。(図 1-13 参照)

②まず最初にアクション１が、先で説明したようにどのような活動に関連づけるかを決め、それが理解しやすいような｢アクション名｣や｢アクション解説｣を決めます。

これを｢ラベル｣に記入します(半角文字換算で最大 32 文字)。入力は任意です。後ほど入力することもできます。
ラベルへ入力した内容は｢ネットワーク監視アクション一覧/設定｣画面に表示されます。

③次にランプの点灯を設定します。

図 1-13 の右図では 5 灯タイプの機種を表しています。3 灯タイプでは青と白の項目は現れません。
アクションで点灯させたいランプの色を選び、｢有効｣にチェックを入れます。

複数のランプを組み合わせたい場合は、それぞれを「有効」にします。「有効」にチェックが入っていないと、動作はしません。
次にランプの点灯速度をプルダウンメニューから選択します。「点灯」・「点滅」・「高速点滅」の三通りから適当なものを選択します。

同様な手順でブザーについても設定してみましょう。

④設定内容は、「テスト実行」ボタンを押して試せます。設定内容に間違いがないか確認します。

点灯の具合やブザーの音量などを確認します。

3 設定内容の反映
画面下部の「設定」ボタンをクリックし、設定値に反映させます。
設定後、アクション一覧に戻ると先ほど設定した内容が、対応する各項にアイコンとして表示されます。

次の STEP 4 で動作テストを行います。次の例をアクション１として設定してみてください。

例： 赤ランプ点灯･緑ランプ高速点滅･ブザー連続鳴動の場合は次のようになります。

図 1-14 アクション設定例

上図アクション１の定義は、「ラベル」には入力がなく、「黄」･「青」･「白」のランプは「有効」にチェックがないので動作対象外の設定で、「赤」ランプは「有効」になっていて「点灯」、「緑」ランプも「有効」で「高速点滅」に設定されていて、同時に「ブザー」は「有効」で「連続」鳴動(PPPPPP……)で動作する設定になっています。

STEP 4 実際に動くか確認してみましょう

4-1 動作テスト

前項までに設定した監視動作とアクションが、実際に動作するか確認してみましょう。

手順

1 設定画面からログアウト

Web 設定ツールの設定画面の左ナビメニューからログアウトを選択し、ログアウトします。画面はモニタ画面に切り替わります。

「状態」部が 正常 であることを確認します。これはすでに「監視対象」の「対象01」に登録された PC に対して死活監視を始めていて、送った信号が正常に帰ってきていることを表しています。

2 動作テスト(正常→異常→正常)

①監視対象に設定した PC の LAN ケーブルを抜きます。

「ネットワーク切断」を擬似的に作り出しました。このとき PC を通して本体の状態を IE で表示していた情報は途絶します(モニタ画面は変化せず直前の情報を表示しています)。

②しばらくすると(監視間隔の設定によって異なる)本体は異常を検知し、STEP 3 のアクション 1 の例で設定した内容(赤ランプ点灯･緑ランプ高速点滅・ブザー連続音)の動作をするか確認します。

③監視対象の PC に、外した LAN ケーブルを再接続し元の状態(①の状態)に戻します。

モニタ画面の警告表示が正常表示に変わり、ランプが OFF になりブザー音が止まることを確認します。

※手動による強制終了

アクションが実行されている途中で、ランプの点灯やブザー音の停止、音声再生を強制終了させたい場合は、本体上面にある「アラームストップボタン」(電源ランプを兼ねた緑ボタン)を動作が停止するまで押し続けます。

異常状態が継続している間、モニタ画面の「状態」カラムの表示は 警告 となります。ただし例では LAN ケーブルを外したので、画面確認ができません。下図を参照してください。(詳細は実践編参照)

図 1-15 [正常]時の表示例(モニタ画面

図 1-16 [警告]時の表示例(モニタ画面)

以上の動作テストをまとめると次の図のようになります。

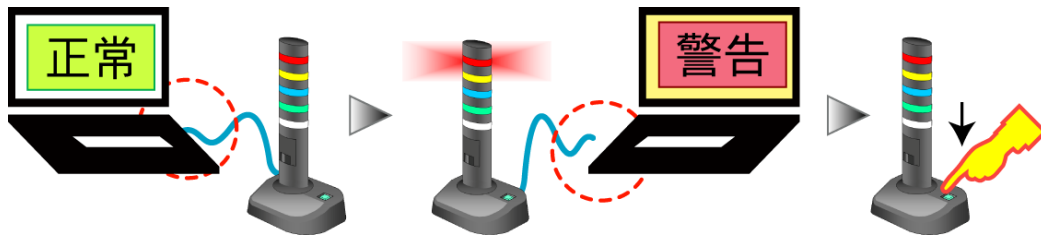



図 1-17 動作テスト概要(まとめ)

4-2 イベントログの確認

異常を検知すると本製品は記録を残します。これを「イベントログ」と記述します。イベントログは、本体の電源が失われても消えることはありません。この記録を読み解くことで、監視対象に何が起こったのかを解析するための一つの情報を提供します。

前項で実行したテストが実際に本製品のイベントログに残っているか確認します。

手順

1 Web ツールへログイン

本体と PC とを LAN ケーブルで再接続しているか確認します。その後、本製品の Web 設定ツールに再度ログインします。ログインについては、前述の STEP3 をご確認ください。

2 メニュー選択

設定画面の左ナビメニューにある「イベントログ」をクリックし、「イベントログ画面」を表示します。

3 ログ確認

イベントログにテスト実行で行ったログ(監視記録)が残っているか確認してください。

次図はその例です。

管理ツール > イベントログ

イベントログ

No.	年月日	時刻	発生イベント
1	2011-12-19	09:32:58	デバイス 1 (192.168.1.5) 警報 On
2	2011-12-17	17:39:47	ツールによるアラーム解除
3	2011-12-17	16:05:01	ツールによるアラーム解除
4	2011-12-17	16:00:16	ツールによるアラーム解除
5	2011-12-17	11:21:47	スイッチによるアラーム解除
6	2011-12-17	11:21:34	デバイス 1 (192.168.1.5) 警報 On

図 1-18 イベントログ画面(ログ内容の例)

イベントログには、発生した順に記録されます(降順、No1.が最新のイベント)。
イベント(障害や監視項目の検知など)は、日付と時間およびその内容を記録しています。
実際の場面では、他の監視装置やシステムに残された障害ログやイベントログと本機のログとを付け合わせ、どのような異常や障害が発生したのかを解析し原因を突き詰めていきます。

これで初歩的な機能や設定方法、監視内容、および動作テストという一連の流れを解説しました。
ご理解いただけましたでしょうか。

この章の最後として、すでに設置場所や設定内容が決定されている場合、IP アドレスを変更登録しておきましょう。
まだ決まっていない場合は、そのままのアドレスでログアウトしましょう。

4-3 設置環境の IP アドレスを設定

「LAN 設定」画面では、本製品のネットワーク情報の設定が行えます。

手順

1 メニュー選択
設定画面左ナビメニューにある「LAN 設定」をクリックし、「LAN 設定画面」を表示します。

2 IP アドレス入力
事前に入手している IP アドレスを入力します。必要に応じてゲートウェイアドレス等を入力します。

3 設定内容の反映
画面下の「設定」ボタンをクリックし、設定値に反映させます。
設定の更新が完了すると、画面上部に「設定を更新しました」のメッセージが表示されます。

その後、Web 設定ツールからログアウトします。

4 一旦ブラウザを閉じます

5 新たに設定した IP アドレスでのログイン確認
本製品を指定された環境に設置し、そのネットワーク環境に LAN 接続し直し、変更した IP アドレスでログインできるか確認ください。
新たなアドレスで Web 設定ツール画面が表示されログインできれば、設置完了です。

次章以降では、監視対象システムや機器に対して本機が持つ多彩な機能や設定方法について説明しています。本機をより深く理解するために引き続きお読みください。

第二章　実践編　– 警子ちゃん 4G 各機能の詳細説明 -

はじめに

本章では、警子ちゃん 4G DN-1500GL シリーズに搭載されている各機能について詳しく解説します。

各機能は関連して動作します。そこで、利用に際して理解したい目的を次のようにまとめ、記述してあります。マニュアルという性質上、タイトルや目次からの検索が必要になるため、それぞれの目的項目には番号が振られています。これらの番号は読む順番を明示してはいますが、実際の利用に当たっては、すでに利用されている警子ちゃん II シリーズや警子ちゃん 3G と類似の部分もあるため、必要箇所を目的に沿って拾い読み・読み飛ばしもできます。

本章での目的別項目分類は次のようになります。

・設置する	設置について	本体を目的の場所に設置する際の説明 無線 LAN モジュールの取付方法
・基本設定する	本体設定 LAN 設定	本体の基本設定項目の説明 ネットワーク設定の説明
・監視する	監視設定 自己監視機能	各種監視方法の設定について説明 本体自身の自己監視について説明
・アクションする	アクション設定 アラーム解除 音声ファイル設定 電子メール設定 SNMP トラップ / コマンド設定	異常検知時の動作設定について説明 アラームの解除方法を説明 音声ファイルの取扱説明 電子メールの設定について説明 SNMP トラップと送出について説明
・外部から制御する	管理ソフトとの連携 アクセス設定 コマンドリファレンス	他のソフトから制御する方法の説明 SNMP v1/v2/v3 からのアクセス方法 コマンド詳細説明
・確認する	確認する	モニタ表示内容の説明 イベントログの説明
・メンテナンスする	メンテナンス	ファームウェアの更新方法 設定データの取扱説明

2-1 設置する

2-1-1 設置条件

次の環境条件に適した、安定した水平な場所に置いてください。

・周囲温度が 45℃以下の室内(20～30℃が望ましい)
・結露しない環境(湿度 20～85%RH)
・水の浸入や水滴落下などで濡れるおそれのない場所
・直射日光の当たらない場所
・塵埃のない場所
・可燃ガス、腐食性ガス、及び霧状の油(オイルミスト)等のない環境
・振動のない場所
・火花や発熱体が近くにない場所
・大容量のモーター等が動作し電圧変動が著しく発生しない場所
・強力な電気、ノイズのない環境

2-1-2 設置と配線

本製品を平坦な場所に設置します。

付属の AC アダプタのケーブルプラグを本体に挿入します。その後 AC アダプタを電源コンセントに挿入します。電源を本体に投入すると、本体正面の緑の押しボタンが点灯し、赤と緑の LED ランプが点滅します。

警子ちゃん 4G には電源スイッチはありません。これは監視装置として機能するため、電源スイッチの投入忘れなどの人為的ミスを排除するためです。

次に LAN ケーブルを本体に接続します。本体をハブやルータなどのネットワーク装置に接続する場合は、ストレートの LAN ケーブルを使います。また警子ちゃん 4G はギガビットイーサネットへの接続が可能です。ネットワーク速度の規格に合ったケーブルを選択します。
ネットワークにつながると、LAN ポートの左右の LED ランプが点滅を始めます。それぞれの LED 点滅の意味は、「第一章 1-1 各部の名称と機能」を参照します。

本体側電源プラグや LAN ケーブルは通常の利用で自然に抜けることはありません。ケーブルが何かの原因で引っ張られ抜けることがないように抜け防止対策を施したい場合は、本体に同梱されている「マウントベース」と「結束バンド」(第一章 1-1 同梱品の確認参照)を下図のように利用して、本体に縛り付けることができます。

抜け防止対策例：
① LAN ケーブル
② AC アダプタケーブル(プラグ)
③ マウントベース
④ 結束バンド

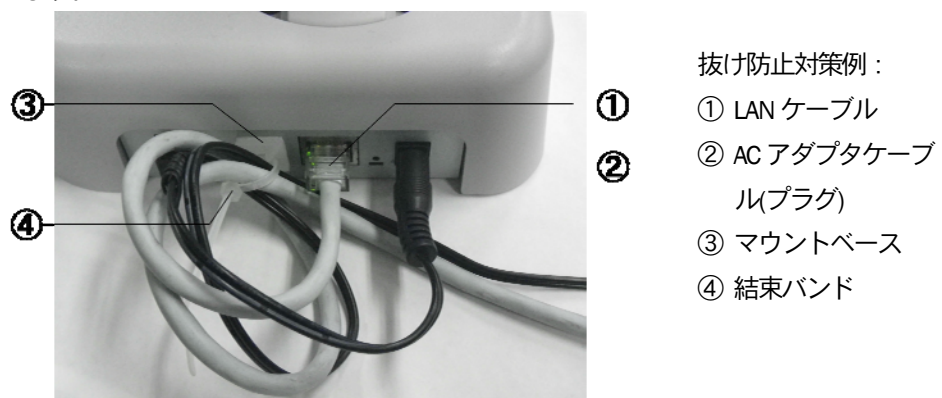



図 2-1 ケーブルの抜け防止対策

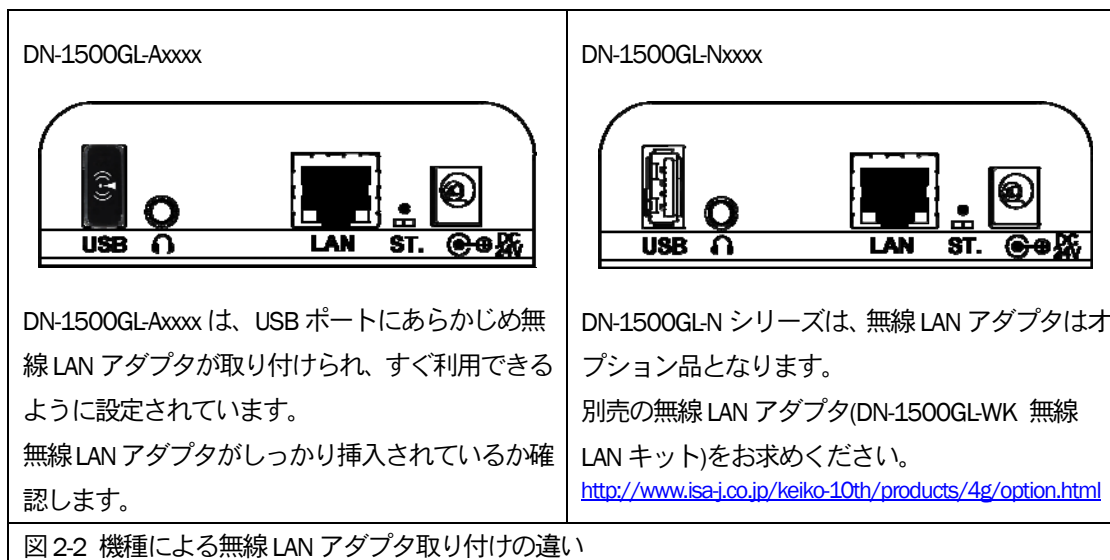
2-1-3 無線 LAN アダプタの取り付け

本製品は専用の無線 LAN アダプタを製品背面の USB ポートに挿入して設置し、無線 LAN 環境につなぐことができます。

警子ちゃん 4G では、無線 LAN アダプタ付きの DN-1500GL-Axxxx と有線 LAN のみの DN-1500GL-Nxxxx があります。

無線 LAN アダプタの取り付けは、本体背面の USB ポートに挿入します。

DN-1500GL-Axxxx	DN-1500GL-Nxxxx
DN-1500GL-Axxxx は、USB ポートにあらかじめ無線 LAN アダプタが取り付けられ、すぐ利用できるように設定されています。 無線 LAN アダプタがしっかり挿入されているか確認します。	DN-1500GL-N シリーズは、無線 LAN アダプタはオプション品となります。 別売の無線 LAN アダプタ(DN-1500GL-WK 無線 LAN キット)をお求めください。 http://www.isa-j.co.jp/keiko-10th/products/4g/option.html

図 2-2 機種による無線 LAN アダプタ取り付けの違い

[注意]

市販の USB 取り付けタイプの無線 LAN アダプタを本機に取り付けても動作しません

2-2 基本設定する

本製品の保守情報の登録や、時刻･管理ユーザの設定などの基本的な本体設定と、LAN ポートや無線 LAN の設定を行います。

基本設定項目は項目が多く、監視内容の変更や移設に伴い見直す項目にもなります。次の表は、各設定項目の掲載ページの一覧です。

2-2-1 本体設定

Web 設定ツールにログインします。
左ナビメニューから「本体設定」を選び、クリックします。

画面は下図のような「本体情報」が表示されます。
必要に応じて各項目に対応する値を設定していきます。

図 2-3 本体情報画面(本体情報)

2-2-1-1 保守契約情報の登録

契約いただいた保守の番号や期限、契約番号を登録できます。

これらの情報を登録することで、技術的な問い合わせや故障判断などの問い合わせの際に、保証契約書を探し抱く手間が省けます。

またお問い合わせいただいた際に、対応窓口で確認のためこれら情報をおたずねします。

契約締結後は送られてくる情報を元に、保守契約情報の登録をお願いいたします。

登録手順は次のようになります。

手順

1. メニュー選択

   画面左ナビメニューの「本体情報」をクリックし、「本体情報」画面を表示します。

2. 設定情報の入力

   手元にある「保守サービス証」を元に、①「保守契約番号」、②「保守契約期限(西暦表記、yyyy/mm/dd 形式)」を入力します。

3. 設定内容の反映

   画面下の「設定」ボタンをクリックし、設定値に反映させます。

2-2-1-2 本体の説明名称を登録する

本体の識別用、あるいは監視目的などの説明名称を登録できます。

登録された内容は、Web 設定ツールのトップ画面に、機器の説明記述として表示します。

手順

1. メニュー選択

   画面左ナビメニューの「本体情報」をクリックし、「本体情報」画面を表示します。

2. 設定情報の入力

   ③「機器説明」に 32 文字以内で入力します。入力は任意で、内容がブランクでもかまいません。

   入力した内容は、web 設定ツールの TOP 画面とモニタ表示画面で確認できます。

3. 設定内容の反映

   画面下の「設定」ボタンをクリックし、設定値に反映させます。

2-2-1-3 Web 動作設定：オートリフレッシュ(自動更新)時間を設定する

Web 設定ツールの画面は Web ブラウザで表示されます。
Web ブラウザは、通常表示内容の更新を自動的に行いません。しかし監視内容を表示するモニタ画面は、常に状況の更新表示が求められます。

そこで本体の Web 動作設定に、一定間隔で表示内容を更新する「オートリフレッシュ」の機能が備わっています。

必要に応じて間隔時間を設定します。変更設定は次の手順で行います。

図 2-4 本体情報画面(Web 動作設定)

手順

1. メニュー選択
   画面左ナビメニューの「本体情報」をクリックし、「本体情報」画面(図 2-4 参照)を表示します。
2. オートリフレッシュ時間の設定
   画面中の「WEB 動作設定」から④「オートリフレッシュ」に、リフレッシュをかける秒数を入力します。
   ※ 10～60 秒の間で指定します。(デフォルト値：10 秒)
   ※ 「0」入力時はオートリフレッシュしません(手動で「内容の再読込み」を実行時)。
3. 設定内容の反映
   画面下の「設定」ボタンをクリックし、設定値に反映させます。

2-2-1-4 Web 動作設定：オートログアウト時間を設定する

Web 設定ツールにログインしたまま離席し、そのままの状態で放置するのはセキュリティ管理上好ましくありません。

そこで本機は、ログインした後何も操作が行われないと「オートログアウト(自動的にログアウト)」する機能を備えています。
分単位の時間を入力し、「オートログアウト」の設定を行います。

手順

1. メニュー選択
   画面左ナビメニューの「本体情報」をクリックし、「本体情報」画面(図 2-4 参照)を表示します。
2. 設定情報の入力
   画面中の「WEB 動作設定」から⑤「オートログアウト」に、オートログアウトする時間を入力します。
   ※ 15 分~30 分の間で指定します。(デフォルト値 : 15 分)
   ※ 「0」入力時はオートログアウトしません。
3. 設定内容の反映
   画面下の「設定」ボタンをクリックし、設定値に反映させます。

2-2-1-5 時刻設定 : 日付と時刻を手入力して設定する

本体に設定された日付と時刻は、異常が発生したときのタイムスタンプとして利用されるため、監視対象の機器類と合わせておくことが必要です。

日付と時刻設定は、必要な情報を手入力で行う方式とシステムが提供する時計サーバ(NTP サーバ)から日付と時刻を一定間隔で取得する方式の設定ができます。

手入力による設定方法は、「第一章　初級編」の「3-3-2 日付と時刻の設定」(13 ページ)で解説してあります。必要な場合、その項を参照します。

※ 本体内蔵のクロックは、キャパシタで停電時でも一定期間保持されます

2-2-1-6 時刻設定 : NTP サーバによる設定

システムに NTP(Network Time Protocol)サーバが提供された場合は、日付や時刻を定期的に同期して、他の同様な機器で起こった事象と本機で残したイベントログとの解析を同一の環境で行うことができます。

※ NTP サーバの情報は、IT 部門が管理している場合が多いので、設置する環境の管理者におたずねください

図 2-5 時刻設定画面(NTP サーバによる設定)

手順

1. メニュー選択
   設定画面左ナビメニュー内「時刻設定」をクリックし、「時刻設定」画面を表示します。
2. 「NTP 機能」の「使用する」にチェック

3. 設定情報の入力
   「問い合わせ先 NTP サーバ」に、アドレスまたは NTP サーバ名を入力します。
   「確認間隔」には、NTP サーバへ情報を取りに行く時間間隔を、プルダウンメニュー(1~24 時間)の中から選択します。
4. タイムゾーンの設定
   本体が設定されている標準時間帯(タイムゾーン)を選択します。タイムゾーンの詳細は次ページを参照してください。
   日本国内は UTC+9 になります。
   ※ UTC：Universal Time, Coordinated
5. 設定内容の反映
   画面下の「設定」ボタンをクリックし、設定値に反映させます。

タイムゾーンとの同期処理について
次の動作で NTP サーバと同期処理が自動的に実行されます。

・時刻設定内、「設定」ボタンをクリックした際
・設定データリストア内、「リストア」ボタンをクリックした際
・電源投入した場合(電源投入後、数十秒後)

サマータイム制度には対応していません。

表 **2-1 NTP** サーバによる時刻設定		
項目名	解説	デフォルト値
NTP 機能	NTP サーバからの情報収集を 有効 / 無効 を設定します	無効
問い合わせ先 NTP サーバ	NTP サーバの IP アドレス、またはサーバ名を入力します。 本製品のカレンダクロックを、指定した NTP サーバに同期させます。	無指定 (空欄)
確認間隔	NTP サーバから情報を取得する時間間隔を指定します	12
タイムゾーン	NTP サーバでカレンダクロック同期の際に参照されます。 日本国内は UTC+9 です。	UTC+ 9

表 2-2 タイムゾーンと主要な国/地域/都市一覧	
タイムゾーン	主要な国/地域/都市一覧
UTC+12	国際日付変更線 東側、フィジー
UTC+11	マガダン、ソロモン諸島、ニューカレドニア
UTC+10	キャンベラ、メルボルン、シドニー、グァム
UTC+9	東京(日本国内)、ソウル、ヤクーツク
UTC+8	北京、重慶、香港、シンガポール
UTC+7	バンコク、ハノイ、ジャカルタ、クラスノヤルスク
UTC+6	アスタナ、ダッカ、ノボシビルスク
UTC+5	エカテリンバーグ、イスラマバード、カラチ、タシケント
UTC+4	アブダビ、マスカット、バク、コーカサス
UTC+3	バグダッド、クウェート、モスクワ、ナイロビ、テヘラン
UTC+2	アンマン、アテネ、ブカレスト、イスタンブール、ベイルート、カイロ、エルサレム
UTC+1	アムステルダム、ベルグラード、ブリュッセル、サラエボ
UTC	協定世界時、ロンドン、モンロビア、レイキャビク
UTC-1	アゾレス諸島、ガーボベルデ諸島
UTC-2	協定世界時-2、中央大西洋
UTC-3	ブラジリア、ブエノスアイレス、カイエンヌ、フォルタレザ、グリーンランド、モンテビデオ
UTC-4	大西洋標準時(カナダ)、ジョージタウン、サンティアゴ
UTC-5	東部標準時(米国及びカナダ)、ボゴタ、リマ、キト
UTC-6	中部標準時(米国及びカナダ)、グアダラハラ、メキシコシティ、サスカチュワン
UTC-7	山地標準時(米国及びカナダ)、アリゾナ、チワワ、ラパス、マサトラン
UTC-8	太平洋標準時(米国及びカナダ)、バハカリフォルニア
UTC-9	アラスカ
UTC-10	ハワイ
UTC-11	協定世界時-11、サモア
UTC-12	国際日付変更線 西側

2-2-1-7 管理ユーザを設定する

「管理ユーザ」とは、本機にログインし様々な設定の管理や変更を行う人です。
この「管理ユーザ」のみが「ユーザ名」と「パスワード」とを入力して本機にログインできるように作られています。

Web 設定ツールの左ナビメニューの本体設定から「管理ユーザ設定」をクリックすると、「管理ユーザ設定」画面(図 2-6 参照)が表示されます。

図 2-6 管理ユーザ設定画面

「ユーザ名」と「パスワード」を入力して、画面下の「設定」ボタンをクリックし、設定を反映します。

工場出荷時の「ユーザ名」と「パスワード」：
ユ ー ザ名：DN1500
パスワード：DN1500

パスワードは間違えるとログインできなくなります。「新しいパスワード再入力」は、コピー＆ペーストを使わず、二度タイプ入力します。

※「ユーザ名」の入力文字制限
半角英数文字と記号の組み合わせで 16 文字以内。大文字、小文字を区別します。
※「パスワード」の入力文字制限
半角英数文字と記号の組み合わせで 16 文字以内。大文字、小文字を区別します。

[注 意]
管理ユーザが登録したユーザ名やパスワードを忘れたような場合、セキュリティ確保の観点から弊社 ISA でも読み出す手段はありません。
しかしログインできないと、工場出荷時の状態にも戻せません。このような状況になった場合は弊社サポート窓口までご連絡ください。

2-2-1-8 アラーム解除設定：アラーム解除を自動/手動に設定する

本機が異常を検知するとアラーム動作の解除方法として次の二通りがあります。

・障害が回復すると自動的にアラームを停止する
・障害が回復してもアラーム動作を継続させ、近傍の作業者に停止ボタンを押させることで手動で強制解除する

図 2-7 アラーム設定画面(アラーム解除方法)

手順

1. メニュー選択
   設定画面左ナビメニュー内「アラーム解除設定」をクリックし、「アラーム解除設定」画面を表示します。
2. 解除方法の選択
   異常回復時にアラーム解除を行う方法を下記より選択します。
   ・ 自動で行う場合は、「自動」
   ・ 手動で行う場合は、「手動」
3. 設定内容の反映
   画面下の「設定」ボタンをクリックし、設定値に反映させます。

2-2-1-9 アラーム解除設定：ストップボタンの動作モードを設定する

本体上面には電源ランプを兼ねた「アラームストップボタン」があります。
このストップボタンを押すことで、アラームを強制的に解除(ランプ、ブザー、音声再生の出力を強制的に OFF に)することができます。

この際ストップボタンの動作は、二つのモードがあります。

モード 1

ボタン押下 1 回目：ブザー音と音声再生を OFF、ランプ点灯は継続。2 回目：ランプを OFF。

図 2-8 ストップボタン動作モード 1

・ブザー(音声)が鳴っていればブザー(音声)だけを OFF にします。
・ブザー(音声)が鳴っていなければランプを OFF にします。

[注　意]
ランプ ON、ブザー(音声)OFF 時に他の監視項目などで異常を検知すると、ブザー(音声)が再度 ON となります。

モード 2

ボタン押下 1 回で全てのランプ点灯とブザー音と音声再生を OFF。

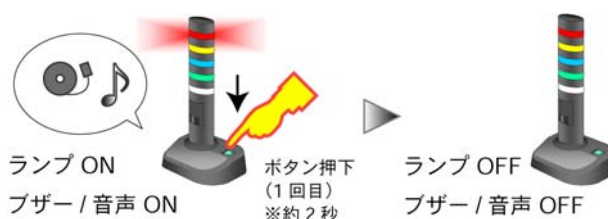



図 2-9 ストップボタン動作モード 2

ランプ、ブザーおよび音声再生すべてが OFF になるまでボタンを押してください(約 2 秒)。

図 2-10 アラーム解除設定(アラーム解除ボタン)

手順

1. メニュー選択
   設定画面左ナビメニューにある「アラーム解除設定」をクリックし、「アラーム解除設定」画面を表示します。
2. アラーム解除(アラームストップ)モードの選択
   先の説明から、運用方法に適したモード１かモード２のどちらかを選択します。

   ※ デフォルトは「モード１」です。

2-2-2 有線/無線 LAN の設定

警子ちゃん 4G は、有線 LAN と無線 LAN がアクセス可能の DN-1500GL-Axxxx と有線 LAN のみの DN-1500GL-Nxxxx があります。

両者の共通の有線 LAN の設定方法から説明します。その後、無線 LAN の設定方法を説明します。また「無線 LAN キット DN-1500GL-WK」を本体に取り付けた後の設定方法は、無線 LAN の設定方法を参照します。

本項では、単に「LAN」は「有線 LAN」を指し「有線」を省略しています。また「有線 LAN」または「無線 LAN」で混同しそうな箇所については、それぞれを省略せず記述しています。

2-2-2-1 LAN 設定：LAN IP アドレスの設定

本製品は IP アドレスとして、IPv4 と IPv6 および両方が混在する「デュアルスタック」に対応しています。
設置する環境に合わせてアドレスを指定します。

図 2-11 LAN 設定画面(LAN IP アドレス設定)

手順

1. メニュー選択

画面左ナビメニュー内「LAN 設定」をクリックし、「LAN 設定」画面(図 2-11 参照)を表示します。

2. 設定情報の入力

利用環境に合わせて、IP アドレス/デフォルトゲートウェイなど設定します。

各項の説明は次の表 2-3 を参照します。

※ 本製品は IPv4 と IPv6 の混在設定が可能です。

※ IPv6 リンクローカルアドレスは自動で生成されます。

3. 設定内容の反映

画面下の「設定」ボタンをクリックし、設定値に反映させます。

[注　意]

有線 LAN と無線 LAN 設定で同じネットワークアドレスを設定できません。

表 2-3 LAN 設定の説明		
項目名	解説	デフォルト値
MAC アドレス	本製品の LAN ポートの MAC アドレス	(機器固有値)
IPv4 アドレス	IPv4 での IP アドレスを入力します。 DHCP サーバによるアドレスを割り当てる場合、「DHCP クライアント」にチェックを入れます。	192.168.1.1
ネットマスク	IPv4 のサブネットマスクです。	255.255.255.0
IPv4 ゲートウェイアドレス	IPv4 のゲートウェイアドレスです。 ルータを越えてネットワークに繋ぐ際、必要になります。	192.168.1.254
IPv6 リンクローカルアドレス	自動で生成されます。	—
IPv6 アドレス	グローバル IPv6 アドレス、又は、ユニークローカル IPv6 アドレスを入力します。	(空欄)
IPv6 ゲートウェイアドレス	IPv6 のゲートウェイアドレスです。 リンクローカルアドレス(FE80::/10)を設定します。ルータ越えてネットワークに繋ぐ際、必要になります。	(空欄)
メトリック	ゲートウェイの優先度を設定します。 有線 LAN と無線 LAN の両ゲートウェイを入力した場合、メトリック値が小さい方が優先的に使用されます。 (1～9999 で指定)	100
通信速度	10Mbps、100Mbps および 1000Mbps を検知し自動で通信速度を設定します(オートネゴシエーション)。	—

2-2-2-2 LAN 設定：無線 LAN IP アドレスの設定

警子ちゃん 4G 無線 LAN 搭載モデル(DN-1500GL-Axxxx)または別売の無線 LAN キット(DN-1500GL-WK)を取り付けた本体を、Wi-Fi 無線 LAN 環境で利用する場合、「無線 LAN IP アドレス」の各項を設定します。

図 2-12 LAN 設定画面(無線 LAN IP アドレス)

手順

1. メニュー選択

画面左ナビメニューの「LAN 設定」をクリックし、「LAN 設定」画面を表示します。
画面をスクロールさせ「無線 LAN IP アドレス」の項を確認します(図 2-12 参照)。

2. 「無線 LAN 有効」にチェック

無線 LAN を利用する場合は、画面の「無線 LAN 有効」にチェックを入れます。

3. 設定情報の入力

利用環境に合わせて、IP アドレス/デフォルトゲートウェイなど設定します。
各項の説明は次の表 2-4 を参照します。

※ 本製品は IPv4 と IPv6 の混在設定が可能です。
※ IPv6 リンクローカルアドレスは自動で生成されます。

4. 表示の確認

IPv6 リンクローカルアドレスが表示されているか確認します。

※ 本製品専用の無線 LAN アダプタが正常に動作していないと、IPv6 リンクローカルアドレスは表示されません。

5. 設定内容の反映

画面下の「設定」ボタンをクリックし、設定値に反映させます。

[注　意]
有線 LAN と無線 LAN 設定で同じネットワークアドレスを設定できません。

表 2-4 無線 LAN 設定の説明

項目名	解説	デフォルト値
無線 LAN 有効	「有効」にチェックすると、無線 LAN を利用可能になります。	無効
MAC アドレス	本製品の無線 LAN ポートの MAC アドレス	(空欄)
IPv4 アドレス	IPv4 での IP アドレスを入力します。 DHCP サーバによるアドレスを割り当てる場合、「DHCP クライアント」にチェックを入れます。	(空欄)
ネットマスク	IPv4 のサブネットマスクです。	(空欄)
IPv4 ゲートウェイアドレス	IPv4 のゲートウェイアドレスです。 ルータを越えてネットワークに繋ぐ際、必要になります。	(空欄)
IPv6 リンクローカルアドレス	自動で生成されます。	—
IPv6 アドレス	グローバル IPv6 アドレス、又は、ユニークローカル IPv6 アドレスを入力します。	(空欄)
IPv6 ゲートウェイアドレス	IPv6 のゲートウェイアドレスです。 リンクローカルアドレス(FE80::/10)を設定します。ルータ越えてネットワークに繋ぐ際、必要になります。	(空欄)
メトリック	ゲートウェイの優先度を設定します。 有線 LAN と無線 LAN の両ゲートウェイを入力した場合、メトリック値が小さい方が優先的に使用されます。 (1～9999 で指定)	100
通信速度	自動で通信速度を設定します(オートネゴシエーション)。	—

2-2-2-3 LAN 設定：DNS サーバアドレスの設定

DNS サーバの指定は、アドレスを指定する方法と DHCP で取得する方法の二通りがあります。

図 2-13 LAN 設定画面(DNS サーバアドレス)

手順

1. メニュー選択

画面左ナビメニュー内「LAN 設定」をクリックし、「LAN 設定」画面を表示します。
画面をスクロールさせ「DNS サーバアドレス」の項を確認します(図 2-13 参照)。

2. 項目にチェック

①既知の DNS サーバを使用するには、
「次の DNS サーバのアドレスを使う」にチェックを入れます。
②DHCP サーバより割り当てる場合
「DNS サーバのアドレスを DHCP で取得する」にチェックします。
※「LAN IP アドレス」または「無線 LAN IP アドレス」設定内の「IPv4 アドレス」項にある、
「DHCP」を選択する必要があります。

3. 設定情報の入力

①プライマリ DNS サーバ(デフォルト値：空欄)
②セカンダリ DNS サーバ(デフォルト値：空欄)
それぞれに IP アドレスを入力します。

※ DNS サーバは IPv4、IPv6 どちらのアドレスも登録できます。

4. 設定内容の反映

画面下の「設定」ボタンをクリックし、設定値に反映させます。

2-2-2-4 LAN 設定：無線 LAN アクセスの設定

無線 LAN IP アドレスの設定が完了した後、設置する無線環境へのアクセス項目を設定します。

図 2-14 LAN 設定画面(無線 LAN アクセス)

手順

1. メニュー選択
画面左ナビメニューの「LAN 設定」をクリックし、「LAN 設定」画面を表示します。
画面をスクロールさせ「無線 LAN アクセス」の項を確認します(図 2-14 参照)。

2. 設定情報の入力
利用環境に合わせて、各項目を設定します。

①「アクティベーションキー」は、付属(書面または本体裏面に貼付)されている「アクティベーションキー」を入力します。
②「SSID」は、「無線 LAN のアクセスポイント識別名」を入力します。
③「暗号化モード」は、無線 LAN アクセスポイントの設定に合わせ、選択します。

※ ③で「WEP」を選択された場合のみ、「暗号強度」以下項目を選択できます。
各項の説明は次の表 2-5 を参照します。

3. 設定内容の反映
画面下の「設定」ボタンをクリックし、設定値に反映させます。

[注　意]
無線 LAN アクセスポイント(親機)の設定情報が必要になります。
事前にネットワーク管理者から無線 LAN の設定情報を入手してください。

表 2-5 無線 LAN アクセス設定の説明		
項目名	解説	デフォルト値
アクティベーションキー	無線LANアダプタに付与されているアクティベーションキーを入力します。製品固有のキーで、これが登録されないと無線 LAN アクセスは有効になりません。 無線 LAN 仕様(型式：DN1500GL-A)の場合： 本体底面貼付のシールを確認ください。 別売の無線 LAN キットの場合： 製品に同梱のアクティベーションキー用紙を確認ください。	(空欄)
SSID	無線 LAN のアクセスポイント識別名 事前に管理者から情報を入手する必要があります。	(空欄)
暗号化モード	無線 LAN アクセスポイント(親機)に設定されている無線 LAN での送受信データの暗号化モードを選択します。 次の 3 種類の暗号化モードから選択します。 ■ Open System ■ WEP ■ WPA/WPA2 - PSK (TKIP/AES) (※) ※ WPA/WPA2-PSK(TKIP)や WPA/WPA2-PSK(AES)は、WPA/WPA2 - PSK (TKIP/AES)を選択してください。	(空欄)
暗号強度	「WEP」を利用する場合： 無線 LAN アクセスポイント(親機)で設定されている暗号強度を選択します。 「64bit」または、「128bit」　から選択できます。	64bit
指定方法	「WEP」を利用する場合： 暗号化キー(解読パスワード)の指定方法を選択します。 下記より選択できます。 ■ 64bit 選択時　文字列(5 桁) 　16 進表記数(10 桁) ■ 128bit 選択時　文字列(13 桁) 　16 進表記数(26 桁)	文字列(5 桁)
WEP キー	「WEP」を利用する場合、無線 LAN アクセスポイント(親機)で設定されている WEP キーを入力します。	(空欄)
WPA 共有キー	「WPA/WPA2 - PSK (TKIP/AES)」を使用する場合は、無線 LAN アクセスポイント(親機)で設定されている WPA 共有キーを入力します。	(空欄)

［注　意］　無線 LAN アダプタ LED（青）について

無線 LAN の設定が有効な場合に、点滅します。

※無線 LAN が有効な場合とは、「無線 LAN IP アドレス」と「無線 LAN アクセス」の設定を行い「無線 LAN 有効」にチェックを入れた場合です。

2-2-2-5 LAN 設定：DHCP 利用による各アドレス設定

本製品は、本機が設置される IT システム環境に DHCP サーバが提供されている場合、それにアクセスして自動的に IP アドレスを取得することができます。

DHCP サーバから取得できる項目は次になります。

・有線 LAN：IPv4 アドレス、サブネットマスク、ゲートウェイアドレス
・無線 LAN：IPv4 アドレス、サブネットマスク、ゲートウェイアドレス
・DNS サーバアドレス

図 2-15 LAN 設定(DHCP を利用する)

手順

1. メニュー選択

画面左ナビメニューの「LAN 設定」をクリックし、「LAN 設定」画面を表示します(図 2-15 参照)。

2. 項目のチェック

DHCP で取得したい項目にチェックをいれます。

IPv4 アドレス(LAN および無線 LAN)の場合：
必要に応じて各項の「DHCP」にチェックを入れます。

DHCP サーバからアドレス情報が取得出来ると、LAN 設定ページを表示した際に設定された IP アドレスが「DHCP」の文字の右側に表示されます（図 2-15 ①参照)。
アドレス情報が取得できたかを確認するには何度か LAN 設定ページを再表示してください。

DNS サーバアドレスの場合：
LAN と無線 LAN の「DHCP」がチェックされていることを確認し、「DNS サーバアドレス」内、「DNS サーバのアドレスを DHCP で取得する」にチェックを入れます。
※ LAN と無線 LAN の「DHCP」いずれかにチェックがされていないと、有効になりません。

2-3 監視する

警子ちゃんシリーズは、対象機器を単独で監視する機能があります。

監視方法は、次の３通りあります。
・IP アドレスで指定された機器に「ping コマンド」を定期的に実行し、その反応をもって監視する死活監視
・対象の機器類から異常状態を表す「SNMP トラップ」信号の有無を監視する状態監視
・自らを監視するウォッチドッグ(watchdog)タイマーと内蔵温度センサによる自己監視

もうひとつ特別な監視として、「アラームストップボタン」の監視機能があります。これは、本機のボタン状態を監視し押されたことをトリガに「アクション」を実行する機能です。人が介在する実質的な運用方法では、「ストップボタン」による動作トリガが非常に有効な場合があります。機能の理解をお勧めします。

※ ping (ピン、ピング)とは：
IP(Internet Protocol)ベースのネットワークにおけるパケットの通達応答性を確認するためのソフトウェアコマンドです。IP の機能が搭載されているほとんどの機器が ping に対する応答性を持っています。一方、セキュリティの観点から、ping に対する応答性はあるが応答する/しないを設定する機器もあります。
対象機器が ping に対して応答できる状態か事前に調べておくとよいでしょう。

※ SNMP(Simple Network Management Protocol)とは：
1990 年に国際的な団体で規格化された仕様で、TCP/IP ネットワークで管理を行うための情報のやりとり(protocol)を定めたものです。

※ SNMP トラップとは：
SNMP を利用したネットワーク管理環境で、管理対象となる機器(SNMP エージェント)から管理サーバ(SNMP マネージャ)に届けられる状況通知のための通信文を送る仕組みです。

※ ウォッチドッグ(watchdog)とは：
本機自体が正常に動作しているかを監視するためのしくみのことです。機器を構成するデバイスやソフトに一定間隔で信号を送らせ、その有無や内容で正常/異常を判断する仕組みです。

監視機能の概念図を次に示します。

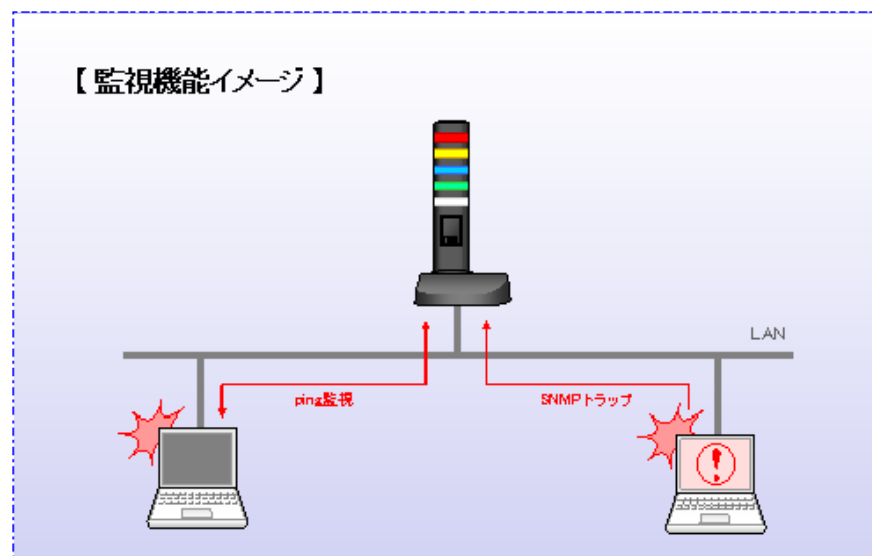



図 2-16 監視機能の概念図

2-3-1 監視設定

ここでは、監視の種類に合わせて設定方法を説明します。

Web 設定ツールにログインします。
左ナビメニューの「監視機能」から、監視する方法に合わせて項目をクリックします。

2-3-1-1 監視設定：ネットワーク死活監視(ping 監視)を設定する

Web 設定ツールの左ナビメニューの「監視機能」から「ネットワーク監視設定」を選択します。
「ネットワーク監視設定」画面が表示されます(図 2-17 参照)。

ネットワーク死活監視は、最大 20 対象を登録することができます。登録は「対象 01」から「対象 05」というように、5 つの登録ごとにページがあり、タイトル直下のタブで切り替えながら登録します。

※ 登録は 1 ページごとに画面下の「設定」をクリックして情報を反映させます。

図 2-17 ネットワーク監視設定画面

手順

1 メニュー選択

設定画面左ナビメニュー内「ネットワーク監視設定」をクリックし、「ネットワーク監視設定」画面を表示します。

2 監視対象の情報入力と登録

監視対象機器の一つを選び(ここでは警子ちゃん 4G の設定画面にアクセスしている PC)、関連情報を次の例を参考に入力していきます。
例では、「対象 01(対象機器番号 01)」を選択しています。ネットワーク監視では最大 20 の監視対象を登録できます。この登録が「対象 01」から「対象 20」に対応します。

図 2-18 ネットワーク監視設定画面(対象 01 設定例)

① 「監視」－「有効」にチェック

監視対象機器に対して監視する/しないを指定します。「有効」にチェックを入れると対象機器の監視が有効になります。逆に「有効」のチェックを外すと、情報は登録されていますが、監視動作はこの機器に対して行われません。

システムの検査や更新時に「有効」のチェックを外します。これにより無用のアクション実行を回避できます。

本製品では対象機器それぞれに対して独立して、「監視」する/しないを設定できます。

② 「説明」には、監視対象機器が理解しやすい名称やコメントを入力します。

ここで登録された「説明」内容は、「web 設定ツールトップ画面(モニタ表示)」の「説明」欄に表示されます。

説明内容は入力してもしなくてもかまいません。「入力が任意」の項目です。ここでは「PC 監視テスト」と入力します。

③ 「アドレス」には監視対象機器の IP アドレスを入力します。

入力できるアドレスは、IPv4 か IPv6 かホスト名のどれかで記述します。

例は、PC でコマンド実行画面を表示させた後、コマンドプロンプトから `ipconfig /all` 等を実行し、監視対象機の LAN ポートに割り当てられた IP アドレス(IPv4)、`192.168.1.5` を入力した状態です。

④ 「監視間隔(秒)」には、監視対象機器に監視信号を送る間隔(秒)を入力します。

監視対象機器の応答特性に合わせ、個別に指定できます。一方で間隔が極端に短いとネットワークトラフィックが増加し、他の機器に影響を与える場合があります。監視対象機器の性質やシステム設計意図などから、適切な値を入力します。

例では、PC の監視を 1 分(60 秒)間に一度監視信号を送り出す設定です。

⑤ 「送信回数」は、上記④で指定された監視間隔内に送る監視信号の回数を指定します。

回数を多くすると、他のネットワーク通信に影響を与える場合があります。

例では 1 回の送出を指定しています。

⑥ 「平均 RTT 閾値」(RTT : Round Trip Time)では、先の④と⑤で監視対象機器に送り出された監視信号が本体に戻ってくるまでの時間をそれぞれの信号について計り、平均値を計算します。

この平均値が指定した時間(対象機器が正常に働いていてもその経路が遅くなったり、故障まではないが反応が遅くなったりする様な場合)を閾(しきい)値として監視します。

ラウンドトリップ時間(RTT)の平均値を監視する場合は、「有効」にチェックを入れ、閾値を指定します。

⑦ **アラートがあがった際のアクションをプルダウンの中から指定します。**

ここで設定する内容は、先に設定した監視対象で異常が発生した(死活信号が帰ってこない、あるいは一定時間内に戻らない等)場合、どのアクション番号で反応し通知するかを紐付けます。
今回は「アクション 1」を選択します。アクションの内容登録は後述してあります。

3 **設定内容の反映**

画面下の「設定」ボタンをクリックし、設定値に反映させます。設定は各ページごとに必要です。
(設定ボタンを押すまでは、本体に記録されません。)

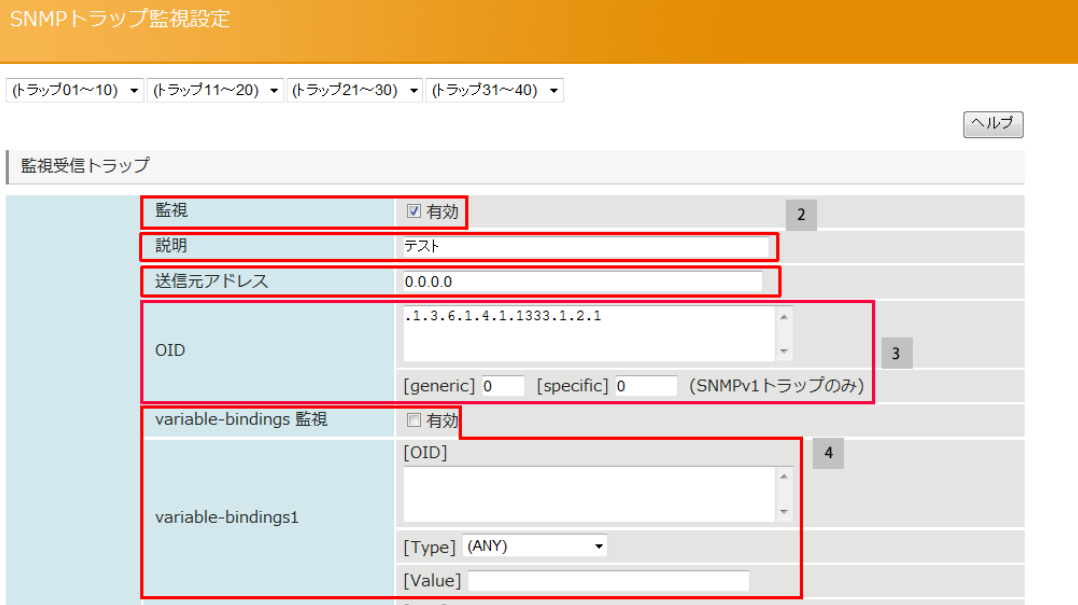



表 2-6 ネットワーク監視設定の説明

項目名	解説	デフォルト値
監視	「有効」にチェックすると、監視を行います。	無効
説明	監視するネットワーク対象の説明を追加したい場合、入力します。(32 文字以内) 入力は任意ですが、識別のため入力を推奨します。	(空欄)
アドレス	監視対象機器の IP アドレスまたはホスト名を登録します。	(空欄)
監視間隔(秒)	対象機器を監視する時間間隔です。秒単位で、15 秒から最大 3,600 秒まで指定できます。 ※ 監視間隔を短めに設定した場合、状況(「監視対象が多い」「異常検出が多い」「アクションが多い」など)により、次回の監視が時間どおり実行できないことがあります。この場合、処理が終了次第、次の監視を実行します。	60
送信回数	1 回の監視確認に対する ping 送信回数を設定します。 (1～99 回) 指定した回数すべてに応答がない場合、エラーと判定します。 ※ LAN トラフィックが非常に高いネットワーク等で通信エラーが多発する場合、この回数を増やす事により不要な異常発報を防ぐことができます。	1
平均 RTT 閾値	ラウンドトリップ時間を判定する場合、有効にチェックを入れ閾値を 1～9,999ms の間で入力します。 ここでの閾値は、「送信回数」で設定した ping 送信回数分のラウンドトリップ時間の平均値です。これを超えた場合に「異常」と判定されます。	無効 1,000 ms
アクション No.	「ネットワーク監視アクション設定」で登録したアクション(次項にて説明)をリストより選択します。	(空欄)

2-3-1-2 監視設定：SNMP トラップ監視を設定する

受信する SNMP トラップを登録しておくことで、トラップ受信をトリガとしたアクションを実行することができます。

登録できる SNMP トラップ数は最大 40 件です。

監視機能 > SNMPトラップ監視設定

SNMPトラップ監視設定

(トラップ01〜10) (トラップ11〜20) (トラップ21〜30) (トラップ31〜40)

ヘルプ

監視受信トラップ

監視 ☑有効 2

説明 テスト

送信元アドレス 0.0.0.0

OID .1.3.6.1.4.1.1333.1.2.1 3

[generic] 0 [specific] 0 (SNMPv1トラップのみ)

variable-bindings 監視 ☐有効

variable-bindings1 [OID] 4

[Type] (ANY)

[Value]

図 2-19 SNMP トラップ監視設定画面

手順

1 メニュー選択

設定画面左ナビメニュー内「SNMP トラップ監視設定」をクリックし、「SNMP トラップ監視設定」画面を表示します。

2 各項の設定

受信トラップの監視を有効にするには「監視」―「有効」にチェックを入れます。

受信トラップに関する説明などを「説明」に 32 文字(半角換算)以内で入力します。入力は任意ですが、監視内容を分かりやすくするため入力を推奨します。

送信元アドレスは、指定した OID を送り出す機器の IP アドレスまたはホスト名を入力します。

3 OID 設定

OID は先頭にピリオドを付加し、ルートから 256 文字以内で記述してください。

例： `.1.3.6.1.4.1.1333.1.2.1`

OID を前方一致で部分的に判定させるには、「*」(アスタリスク)を指定します。「*」はワイルドキャラクタとかワイルドカード呼ばれ、それ以降にどのような文字や文字数であっても「*」1 文字で表現できます。

すなわち、「*」を指定した場合は直前の OID 番号までが一致(前方一致)するもの全てとなります。

例：トラップの OID 指定が `.1.3.6.1.4.1.1333.1.2.6.4.*`の場合は、「*」以前の OID 一致のみを判定します。

`.1.3.6.1.4.1.1333.1.2.6.4.1` や `.1.3.6.1.4.1.1333.1.2.6.4.1.2.0` など `.1.3.6.1.4.1.1333.1.2.6.4` まで一致するものは全てという指定になります

※SNMPv1 トラップの受信では、generic-trap, specific-trap を識別する場合は、generic,specific の欄を設定します。識別する必要のない場合は空欄にしてください。

generic: OID の trap type(0～6)を指定します。Specific を指定する場合は、6 を入力します。
0～5 の一般トラップを設定する場合は specific は空欄にしてください。

specific：vendor specific を指定します(0～2147483647)。
specific だけを入力した場合は、generic に自動的に 6 が設定されます。

※SNMPv2 トラップの受信では generic, specific は空欄にしてください。

OID(Object ID)とは：
SNMP における一つ一つのオブジェクトに振られた識別子を意味します。個々の管理情報や種類を識別するための一種の名前の様なものです。互換性を確保するための共通のオブジェクトと機種固有の機能に合わせたオブジェクト ID とがあります。

4 variable-bindings の設定

variable-bindings の監視を有効にするには、「variable-bindings 監視」－「有効」にチェックをいれ、判別したい variable-bindings の OID(インスタンス)を 256 文字以内で入力し、その variable-bindings の Type と Value を選択します。

OID(インスタンス)の記述例
例： `.1.3.6.1.4.1.1333.1.2.1`

「*」を使って OID を記述すると、「*」はワイルドキャラクタとなり、それより前の記述に一致するもの全てが該当します。(詳細は、先の「 3 OID 設定」を参照してください)

variable-bindings とは：
最近の機器では運用管理を的確に行う目的で、SNMP トラップの通知をいくつかの識別子と値を組み合わされます。この組を variable-bindings といいます。

[参　考]

variable-bindings 監視について、variable-bindings を多数内包するトラップについては 40 番目までが監視対象となります。
41 番目以降は検知できませんので注意してください。

[参　考]

variable-bindings で文字列を判定する場合、文字列に改行コードの制御コードが含まれる場合は、
改行コードより以前の文字列が判定対象になります。
設定の際は Value 欄に改行コードより以前の文字列を設定してください。

5 アクション選択

登録したトラップを受信した際に、実行するアクションを選択します。
アクションの内容は、後述の「SNMP トラップ監視アクション一覧」で設定します。

6 設定内容の反映

画面下の「設定」ボタンをクリックし、設定値に反映させます。

表 2-7 監視受信トラップ設定の説明

<table>
<tr><th>項目名</th><th colspan="2">解説</th><th>デフォルト値</th></tr>
<tr><td>監視</td><td colspan="2">「有効」にチェックすると、監視を行います。</td><td>無　効</td></tr>
<tr><td>説明</td><td colspan="2">受信トラップに関する説明などを入力します。(32 文字以内)
入力は任意です。</td><td>(空　欄)</td></tr>
<tr><td>送信元アドレス</td><td colspan="2">登録されたIPアドレスから送信されたSNMPトラップを受信した時のみアクションを実行します。
※ 送信元の IP アドレスを識別する必要ない場合は、空欄に。</td><td>(空　欄)</td></tr>
<tr><td rowspan="3">OID</td><td colspan="2">登録されたOIDのSNMPトラップを受信した時のみアクションを実行します。
OID を識別する必要のない場合は空欄にしてください。
OID の長さは最大 256 文字です。</td><td>(空　欄)</td></tr>
<tr><td>generic</td><td>OID の trap type(0～6)指定します。
Specific を指定する場合は、6 を入力します。
generic を識別する必要のない場合は空欄にしてください。</td><td>(空　欄)</td></tr>
<tr><td>specific</td><td>vendor specific を指定します。(0～2147483647)
specific を識別する必要のない場合は空欄にしてください。</td><td>(空　欄)</td></tr>
<tr><td>variable-bindings 監視</td><td colspan="2">「有効」にチェックすると、variable-bindings 監視を行います。</td><td>無　効</td></tr>
<tr><td>variable-bindings OID</td><td colspan="2">variable-bindings の OID(インスタンス)を入力します。
最大５件まで登録できます(AND 条件)。OID の長さは最大 256 文字です。</td><td>(空　欄)</td></tr>
<tr><td>variable-bindings Type</td><td colspan="2">「(ANY)」・「Integer32」・「OBJECT_ID」・「OCTET STRING」の中から、Value の型を選択します</td><td>(ANY)</td></tr>
<tr><td>variable-bindings Value</td><td colspan="2">Value を設定します(32 文字以内)
(ANY)：　半角英数字と_@-.:/()
Integer32：　半角数字　-2^31～2^31-1
OBJECT_ID：　半角数字とピリオド
OCTET STRING：　文字列(ASCII 文字列･32 文字以内)</td><td>(空　欄)</td></tr>
<tr><td>アクション選択</td><td colspan="2">「SNMP トラップ監視アクション一覧定」で登録したアクションをリストより選択します。</td><td>(空　欄)</td></tr>
</table>

[参　考]
トラップの判定はトラップ 01 から順に行われ、設定に一致するトラップが検出された場合は以降の設定内容の判定を行いません。

[参　考]
SNMP トラップ受信によって実行されたアクションの解除は、解除を指示するトラップの受信以外に３通りの方法があります。
詳細は、「アクションする」の「アラーム解除」の項を参照します。

2-3-1-3 監視設定：アラームストップボタン監視を設定する

本体上部にある、電源ランプを兼ねた緑色の押しボタンスイッチが「アラームストップボタン」です。

アラームストップボタンは、単にランプの点灯やブザー音および音声ファイルの再生を無効にするだけでなく、押されたときにアクションを実行するように設定することができます。

この機能は、たとえば回復作業が終了した合図に利用したり、異常状態を確認した人がネットワーク上にSNMP トラップを上げたりするのに利用すると便利です。

アクションとして設定できる機能は、電子メール送信、SNMP トラップ送信、コマンド実行の３通りで、これらを単独あるいは組み合わせることができます。

手順

1 メニュー選択

設定画面左ナビメニュー内「アラーム解除設定」をクリックし、「アラーム解除設定」画面を表示します。

2 監視有効の設定

アラームボタン監視の「監視」—「有効」にチェックします。

3 画面の表示

「アラームストップボタンアクション」の「アクション設定」をクリックし、「アラームストップボタン監視アクション設定」画面を表示します。

図2-20 アラームストップボタン監視アクション設定画面

4 アクションの設定

実行させたいアクションをそれぞれ設定します。各項目は以下項を参照。

※　各アクションを有効にする場合は、各「有効」にチェックをいれます。

「メール送信」：	「ネットワーク異常時にメールを送信する」
「SNMP トラップ通知」：	「ネットワーク異常時にSNMP トラップ通知する」
「コマンド実行」：	「異常時、または回復時にコマンドを実行する」

5 設定内容の反映

画面下の「設定」ボタンをクリックし、設定値に反映させます。

2-3-2 自己監視機能

警子ちゃん 4G では、ネットワーク環境や設置環境の変化等から影響を受けた場合、自らを二つの機能で自己監視機能を利用して復帰を試みます。

設定する項目は特にありません。

自己監視機能が働き、本体が再起動したり SNMP トラップを送信した形跡は、イベントログに記録されます。記録されるログの詳細は、付録を参照します。

2-3-2-1 自己監視機能：ウォッチドッグ

ウォッチドッグとは、本機自身が正常に動作しているかを監視するためのしくみです。本機では、機器を構成する内部回路やソフトに対して一定間隔で常に信号を送り、その有無や内容で正常/異常を判断し、異常と判断すると「ハングアップ」したものとして、自動的に再起動し「イベントログ」に記録されます。

本体が正常に動作しているときは、本体裏面のステータスランプ(STATUS LED、緑の LED)が一定間隔で点滅します。

①	WatchDog (緑 LED)	正常時　　点滅
②	未使用	

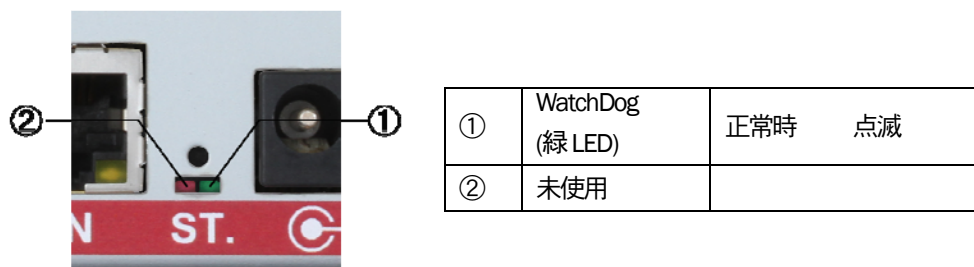



図 2-21 STATUS LED

2-3-2-2 自己監視機能：内部温度監視

警子ちゃん 4G は、温度センサを筐体内に設け内部温度を監視しています。

本機は低消費電力タイプのプロセッサを利用しています。この利点は、冷却のためのファンなど長期間使用する際の故障原因になる部品は極力使用せず信頼性を維持することができます。

一方、本体が設置されている環境温度が上がるとその影響で筐体内の温度が上昇します。実測では周辺温度(動作温度)に対して約 15℃程度高くなる場合があります。この対策として、筐体下部を放熱効果の高い金属と構造などで構成しています。

しかし、設置底面が機器の放熱等で局所的に高くなることも想定されるため、筐体内部温度が約 70℃(動作保証温度上限値＋10℃程度の環境での内部温度を想定)を超えると、事前に設定されている通知先に SNMP トラップを送信し、異常を知らせます。

2-4 アクションさせる

警子ちゃんシリーズは、監視機能で異常を検知すると周辺の人やネットワークを通して他の装置に伝達する「アクション」機能があります。

※ アクションとは：

ランプを点灯させたりブザーを動作させたり、また音声ファイルを再生し周囲で作業する人たちに異常を伝達する、あるいはネットワークを通し電子メールやSNMP トラップを送信したり、他の機器に対してコマンドを発行する「通知動作」をいいます。

(「待機点灯」を設定している場合、ランプのアクションに制限があります)

アクションの種類は、次の６通りあります。

・LED ランプの点灯・点滅・消灯
・ブザーの作動
・音声ファイルの再生
・電子メールの送信
・SNMP トラップの送信
・コマンドの実行

これらのアクションは単独あるいは組み合わせて設定できます。また監視状態が「異常」から通常状態に「回復」したときのアクションも設定できます。本書では、これを「回復アクション」と記述する場合もあります。

本項では、先に「アクション」の設定方法を説明します。それに続き、各アクション機能の準備や設定について説明します。

本項と次項「2-5 準備・設定する」で説明する内容は、次のものです。

本項「2-4 アクションさせる」で説明：

アクション設定	ネットワーク死活監視(Ping 監視)のアクションを設定する
	SNMP トラップ監視のアクションを設定する
	アクション実行時警報(ランプ・ブザー・音声)を設定する
	異常時にメールを送信する
	異常時にSNMP トラップ通知する
	異常時、または回復時にコマンドを実行する
アラーム解除	アラームを解除する

次項「2-5 準備・設定する」で説明：

音声ファイル設定	音声ファイル設定
	音声ファイルを登録する
	登録した音声ファイルを視聴する
	音声ファイルのバックアップ
	音声ファイルデータのリストア
電子メール設定	電子メール設定
	電子メールを設定する
	送信するメールの内容を設定する　(アクション内容設定)
	イベントログをメールで送信する

SNMP トラップ/コマンドの設定

SNMP の設定

SNMP トラップによる通知先の設定

実行コマンドの内容を設定する

TCP ソケット通信の設定

待機点灯の設定

2-4-1 アクション設定

アクション設定は、次の３つの監視機能に対して設定できます。

・「ネットワーク死活監視」
・「SNMP トラップ監視」
・「アラームストップボタン監視」

実行可能なアクションは、次の図のように６種類です。

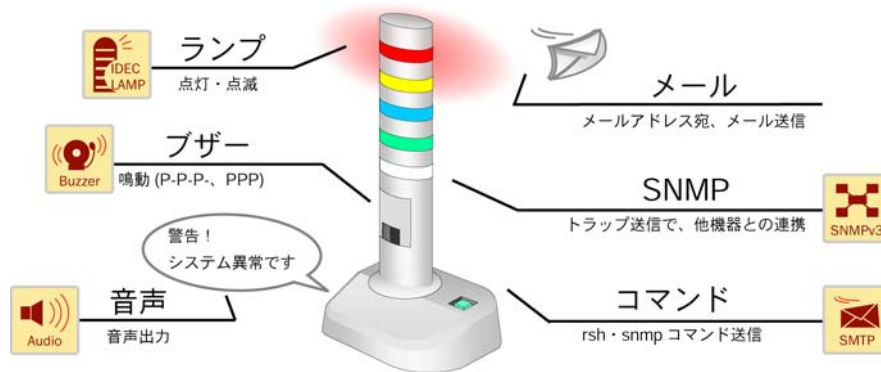



図 2-22 実行可能な６つのアクション

[注　意]

「アラームストップボタン監視」では、ランプの点灯･点滅、ブザー動作、音声ファイルの再生の３つのアクションは実行できません。

2-4-1-1 アクション設定：ネットワーク死活監視(ping 監視)のアクション設定

本マニュアルを初級編から読まれた方はすでに、この項で説明する内容は体験済みです。

初級編 STEP３の「3-4-2 アクションの設定　～ランプ・ブザー・音声の設定～」で簡単な例を実際に設定しました。

ネットワーク死活監視(ping 監視)対象機器から異常･回復を検知した時に、実行するアクションを設定します。登録できるアクションの種類は最大 20 件です。

「ネットワーク監視アクション一覧」から、各アクションの設定画面を表示し、ランプ点灯･ブザー音など実行するアクションを設定します。

※ 同じ内容のアクションを複数の監視対象に設定すると、異常の見分けが付きにくくなります。一方で、運用ルールなどが決められる場合は、そのルールとアクションとを関連づけることで、複数の監視対象のアクションを同じ内容に設定する場合もあります。

手順

1　メニューの選択

設定画面左ナビメニュー内「ネットワーク監視アクション一覧/設定」をクリックし、「ネットワーク監視アクション一覧」画面(図 2-23 の左図を参照)を表示します。

※「アクション一覧」では設定された内容を確認するために、「ネットワーク監視アクション設定」(図 2-23 の右図)で設定された内容が表示されます。

図 2-23 ネットワーク監視アクション一覧(アクション一覧、アクション設定)

2　アクション設定の選択

設定したいアクション番号のボタンをクリックし(図 2-23 の左図を参照)、各「ネットワーク監視アクション設定」画面(図 2-23 の右図)を表示します。

3　ラベルの入力

アクションの名前を設定します。(半角換算 32 文字以内、入力は任意)

4　アクションの設定

アクションを設定します。

※ 各アクションの設定は、それぞれの項に説明を引き継ぎます。

同一ランプに対して状態の異なるアクション設定を行った場合、
アクション実行時のランプの状態は、【　高速点滅 > 点滅 > 点灯 】の優先順位となります。

※SNMP トラップ監視の場合は、【　消灯 > 高速点滅 > 点滅 > 点灯 】の優先順位となります。

ブザー音に対して状態の異なるアクション設定を行った場合、
アクション実行時のブザー音の状態は、【　連続 > 断続　】の優先順位となります。

※SNMP トラップ監視の場合は、【　連続 > 断続　】の優先順位となります。

2-4-1-2 アクション設定：SNMP トラップ監視のアクション設定

SNMP トラップ監視対象機器から異常･回復を検知した時に、実行するアクションを設定します。
登録できるアクションの種類は最大 40 件です。

「SNMP トラップ監視アクション一覧」から、各アクションの設定画面を表示し、ランプ点灯･ブザー音など実行するアクションを設定します。

※ 同じ内容のアクションを複数の監視対象に設定すると、異常の見分けが付きにくくなります。一方で、運用ルールなどが決められる場合は、そのルールとアクションとを関連づけることで、複数の監視対象のアクションを同じ内容に設定する場合もあります。

手順

1 メニューの選択
設定画面左ナビメニュー内「SNMP トラップ監視アクション一覧/設定」をクリックし、「SNMP トラップ監視アクション一覧」画面(図 2-24 の左図を参照)を表示します。

※「アクション一覧」では設定された内容を確認するために、「SNMP トラップ監視アクション設定」(図 2-24 の右図)で設定された内容が表示されます。

図 2-24 SNMP トラップ監視アクション一覧(アクション一覧、アクション設定)

2 アクション設定の選択
設定したいアクション番号のボタンをクリックし(図 2-24 の左図を参照)、各「SNMP トラップ監視アクション設定」画面(図 2-24 の右図)を表示します。

3 ラベルの入力
アクションの名前を設定します。(半角換算 32 文字以内、入力は任意)

4 アクションの設定
アクションを設定します。

※ 各アクションの設定は、それぞれの項に説明を引き継ぎます。

2-4-1-3 アクション設定：ランプ、ブザーの設定

警子ちゃん4Gは、警子ちゃん3Gから採用された高輝度LEDランプ·ブザーを採用しています。

ランプ灯数は、３灯モデル(赤、黄、緑)と５灯モデル(赤、黄、緑、青、白)があります。機種により設定画面に現れるLEDランプの項目は変わります。
ランプの点灯方式は、「消灯」、「点灯」、「点滅」および「高速点滅」があります。

ブザーは音程が１種類です。警告の伝達と遠くまで通ることを目的としているため、国際規格に則った「耳障りな音」になっています。
ブザー音は、「連続音(PPPP･･･)」、「断続音(P―P―P―P―･･･)」および「停止」があります。

これらを一つのアクションに組み合わせて設定ができます。

通常状態の時、常にランプ（3灯の場合は緑、5灯の場合は緑・青・白から１色）を点灯または点滅させ、異常時は指定されたランプを消灯する「待機点灯」という機能があります。
詳細は「2-5-6　待機点灯の準備」を参照ください。

手順

1 メニューの選択

設定画面左ナビメニュー内「ネットワーク監視アクション一覧/」設定」(図2-25参照)または「SNMPトラップ監視アクション一覧/設定」(図2-26参照)をクリックし、「アクション一覧」画面を表示します。
※ 図では５灯モデルでそれぞれの監視に対してアクション01に設定する例を示しています。

図2-25 ネットワーク監視アクション設定(ランプとブザー)

図 2-26 SNMP トラップ監視アクション設定(ランプとブザー)

2	設定の有効

動作させたい項目(ランプ／ブザー)の「有効」にチェックし、ランプおよびブザーの動作パターンをリストから選択します。

3	設定内容の反映

画面下の「設定」ボタンをクリックし、設定値に反映させます。

表 2-8 アクション(ランプ、ブザー)設定の説明

項目名	解説	デフォルト値
ランプ	各ランプの動作を「有効」にチェックを入れて選択します。 灯数モデルで 3 灯(赤、黄、緑)、5 灯(赤、黄、緑、青、白)を選択します。 「点滅」(約 30 回/分で点滅)、「点灯」(点灯継続)、「高速点滅」(約 60 回/分で点滅)で各の点灯パターンを選択します。 ※ SNMP トラップ監視アクション設定には、上記項目に「消灯」が加わります。	(無　効) (点　灯)
ブザー	ブザーの動作を「有効」にチェックを入れて選択します。 「連続」(PPPP･･･、約 700 回/分)、「断続」(P—P—P—P—･･･、約 35 回/分)の選択ができます。 ※ 音程は、約 3.3kHz で、音量調整はランプ部全面のノブで 70~90dB の調整ができます。 ※ SNMP トラップ監視アクション設定には、上記項目に「停止」が加わります。	(無　効) (連　続)

2-4-1-4 アクション設定：音声ファイルの再生

警子ちゃん 4G の新しい機能として、音声ファイルの再生がアクションとして実行できます。
音声信号は、本体後面の「Audio コネクタ(ミニジャック)」端子から出力されます。出力レベルはヘッドホンで聞ける程度で、本体から直接音を聞けません。従って、警告音として利用するためには、外部拡声装置(PC 用の外部アンプ･スピーカ装置など)に接続します。本体と外部装置に接続するためのケーブルは付属しません。機器にあわせて別途用意します。

※ PC の「マイク入力」に接続することはできますが、インピーダンスが整合してないため信号レベルが極端に低くなることがあります。「入力レベルの調整」などを使って、事前に試してください。

※ PC の「ヘッドフォン端子」に間違って接続すると本体が壊れる場合があります。接続には事前に十分注意して行います。

音声ファイルは、最大 20 個(あるいは登録ファイル容量の合計が 10Mbyte 以下)の登録が可能です。電源が切れても登録された音声ファイルは消えません。

サンプルの音声ファイルが 2 つ登録されています。
操作の習得や実際の運用でご利用いただけます。なお、音声ファイルは著作権の対象です。警子ちゃん 4G での利用に限定されています。他の機器での再生はご遠慮ください。

音声ファイル再生のアクションは、先のランプやブザーのアクションと平行して実行されます。すなわち、ランプが点灯し、ブザーが鳴り、音声が再生されるが同時にできます。

音声ファイルの再生は、音声ファイルが内容により長さに左右されることを想定し、あるいは気づくまでの時間を確保する目的で、繰り返し回数が指定できます。

手順

1 メニューの選択

設定画面左ナビメニュー内「ネットワーク監視アクション一覧/｣ 設定｣ (図 2-27 参照)または「SNMP トラップ監視アクション一覧/設定｣ (図 2-28 参照)をクリックし、「アクション一覧」画面を表示します。

図 2-27 ネットワーク監視アクション設定(音声ファイルの再生)

図 2-28 SNMP トラップ監視アクション設定(音声ファイルの再生)

2 設定の有効

アクション「音声」－「有効」にチェックを入れ、出力したい音声ファイルを選択します。

音声は「連続再生」または「再生回数(1～99 回)を指定します。

3 設定内容の反映

画面下の「設定」ボタンをクリックし、設定値に反映させます。

表 2-9 アクション(音声ファイルの再生)設定の説明		
項目名	解説	デフォルト値
音声	音声ファイルの再生は、「有効」にチェックを入れて選択します。 音声 1～20 があります。 ※ 音声 1～2 にはサンプル音声が登録されています。不要の場合は、削除できます。削除する際は、事前にバックアップの作成をお勧めします。 ※ SNMP トラップ監視アクション設定には、上記項目に「停止」が加わります。	(有　効) (1:警告、警告～)
音声の出力回数	指令された音声ファイルの再生回数を指定します。リピートは「連続」または「回数指定(1～99 回)」で指定できます。 ※ 「連続」にチェックした場合、「警報が解除されるまで」または「アラームが解除されるまで」なり続けます。	(1 回)

2-4-1-5 アクション設定：電子メールの送信

「ネットワーク死活監視」、「SNMP トラップ監視」および「アラームストップボタン監視」のアクションとして、事前に設定した内容を指定した宛先に「電子メール」で送信します。

手順

1 メニューの選択

設定画面左ナビメニュー内「SNMP トラップ監視アクション一覧/設定」、「ネットワーク監視アクション一覧/設定」(図 2-29 参照)または「アラーム解除設定」(図 2-30 参照)をクリックし、「アクション一覧(設定)」画面を表示します。

図 2-29 ネットワーク監視アクション設定(電子メールの送信)

図 2-30 アラームストップボタン監視アクション設定(電子メールの送信)

2 設定の有効/メール内容の設定

アクションの設定は、「メール送信」－「有効」にチェックを入れます。

通知したい「メール内容」(「登録された件名」を表示)を、リストより選択します。

※ 電子メールの内容設定は、別項目で解説しています。

3　メール送信先の指定

事前に登録したメール送信先(最大５件)から通知したいメール送信先に、チェックを入れます。

4　設定内容の反映

画面下の「設定」ボタンをクリックし、設定値に反映させます。

2-4-1-6 アクション設定：SNMP トラップ通知

「ネットワーク死活監視」、「SNMP トラップ監視」および「アラームストップボタン監視」のアクションとして、事前に設定した内容の「SNMP トラップ」を送信します。

手順

1　メニューの選択

設定画面左ナビメニュー内「SNMP トラップ監視アクション一覧/設定」(図 2-31 参照)、「ネットワーク監視アクション一覧/設定」または「アラーム解除設定」(図 2-32 参照)をクリックし、「アクション一覧(設定)」画面を表示します。

図 2-31 SNMP トラップ監視アクション設定(SNMP トラップ通知)

図 2-32 SNMP トラップ監視アクション設定(SNMP 通知)

2 設定の有効

「SNMP トラップ通知」—「有効」にチェックを入れます。

3 設定内容の反映

画面下の「設定」ボタンをクリックし、設定値に反映させます。

2-4-1-7 アクション設定：コマンド実行

「ネットワーク死活監視」、「SNMP トラップ監視」および「アラームストップボタン監視」のアクションとして、事前に設定･登録した内容の「コマンド実行」を実行します。

「ネットワーク死活監視」と「SNMP トラップ監視」では、「異常時コマンド実行(異常を検知したときに実行するコマンド)」と「回復時コマンド実行(回復を検知したときに実行するコマンド)」を設定できます。

「アラームストップボタン監視」では、「ボタン押下時コマンド実行(ボタンの押し下げを検知して実行するコマンド)」と「ボタン解放時コマンド実行(ボタンを押し下げから放したことを検知して実行するコマンド)」を設定できます。

それぞれ運用ルールに合わせて利用します。

手順

1 メニューの選択

設定画面左ナビメニュー内「SNMP トラップ監視アクション一覧/設定」、「ネットワーク監視アクション一覧/設定」または「アラーム解除設定」をクリックし、「アクション一覧(設定)」画面(図 2-33 参照)を表示します。

図 2-33 アクション設定(コマンド実行)

2　設定の有効

該当する「コマンド実行」－「有効」にチェックを入れ、実行コマンドをリストより選択します。

3　設定内容の反映

画面下の「設定」ボタンをクリックし、設定値に反映させます。

2-4-2 アラーム解除

アラームを強制的に解除する方法は、次の３通りあります。

※「アラーム」とは、ランプの点灯、ブザー鳴動、音声ファイルの再生のどれか、または複数の機能の動作を言います。

※「待機点灯」が設定されている場合、アラーム解除と当時に元の「待機点灯」状態に戻り、指定されている表示灯が点灯します。

2-4-2-1 アラーム解除 : Web 設定ツールから

web 設定ツールのメニュー「アラーム解除設定」画面内「全アラーム解除実行」ボタンをクリックします。

※ アラームストップボタンのモードに関係なく、１クリックで**全アラーム(ランプ/ブザー/音声)**が一斉解除されます。

図 2-34 全アラーム解除実行(web 設定ツールから)

2-4-2-2 アラーム解除：アラームストップボタンから

本体筐体上部の「アラームストップボタン」をアラームが停止するまで、ボタンを押し下げ続けます(約２秒)。

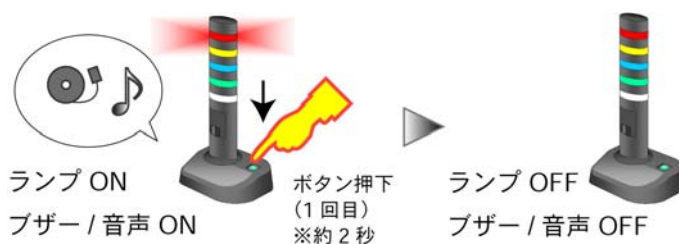



図 2-35 アラーム解除(アラーム解除ボタンから)

2-4-2-3 アラーム解除：コマンド実行

リモートシェルの「ALOF コマンド」または、SNMP コマンドの「objectName：ctrlALOF コマンド」を実行します。

※「リモートシェルコマンド」と「SNMP コマンド」については後述してあります。

図 2-36 アラーム解除(コマンド実行)

2-5 準備･設定する

この節では、音声ファイルの準備と電子メールの設定、電子メールの内容の準備や設定、SNMP トラップ通知の準備や設定、外部機器やアプリケーションから直接制御する際のコマンド実行の準備や TCP ソケット通信の準備、正常時に待機状態を明示的に表示させる待機点灯の設定について説明します。

2-5-1 音声ファイルの準備

警子ちゃん 4G の新しい機能として、音声ファイルの登録、再生、バックアップができます。

音声ファイルは、最大 20 個(あるいは登録ファイル容量の合計が 10Mbyte 以下)の登録が可能です。電源が切れても登録された音声ファイルは消えません。

サンプルの音声ファイルが 2 つ登録されています。
操作の習得や実際の運用でご利用いただけます。なお、音声ファイルは著作権の対象です。警子ちゃん 4G での利用に限定されています。他の機器での再生はご遠慮ください。

音声ファイルのフォーマットは、MPG3(MPEG3 や MP3 と記述する場合もあります)です。
市販のデジタルボイスレコーダで録音し、PC 等に取り込み、市販あるいはフリーの音声編集ソフトを利用して、MPG3 フォーマットに変換することで、簡単に自由に本機用の音声ファイルを制作することができます。
また音声編集ソフトの中には、複数の音声ファイルを連結して一つの音声ファイルに統合するものもあります。この機能を使えば、主語、目的語、動詞を別々に録音し、編集段階で組み合わせすることで多くの音声ファイルを作ることができます。

MPG3 の音声ファイルは、多くの場合圧縮することができます。一般的には、圧縮度と音質とは反比例します。用途に合わせて圧縮度を選択します。

音声ファイルの再生信号は、本体後面の｢Audio コネクタ(ミニジャック)｣端子から出力されます。出力レベルはヘッドホンで聞ける程度で、本体から直接音を聞くためのアンプやスピーカは内蔵していません。従って、警告音として利用するためには、外部拡声装置(PC 用の外部アンプ･スピーカ装置など)に接続します。本体と外部装置に接続するためのケーブルは付属しません。機器にあわせて別途用意します。

※ PC の｢マイク入力｣に接続することはできますが、インピーダンスが整合してないため信号レベルが極端に低くなることがあります。｢入力レベルの調整｣などを使って、事前に試してください。

※ PC の｢ヘッドフォン端子｣に間違って接続すると本体が壊れる場合があります。接続には事前に十分注意して行います。

音声ファイルは、PC から自由に本体に登録、削除、バックアップができます。

2-5-1-1 音声ファイルの準備：音声ファイルの登録

本製品では、最大 20 の音声ファイルを登録し、アクション時に事前に登録した音声ファイルを指定して再生することができます。

※ 音声ファイルの登録は、全容量の合計が 10Mbyte 以下です。

音声ファイルの登録方法を次に説明します。

手順

1　メニュー選択

設定画面左ナビメニュー内「音声ファイル登録」をクリックし、「音声ファイル登録」画面(図 2-37 参照)を表示します。

図 2-37　音声ファイルの登録

2　ファイル名の登録

「音声ファイル登録」ボタンをクリックし、「音声ファイル登録」画面(図 2-37 参照)を表示します。「音声ファイルのパス」―「ファイルを選択」ボタンをクリックし、登録するファイルを選択します。「タイトル」を入力します。入力は任意です。

※ タイトル名を空欄にした場合は、ファイル名がタイトル名に反映されます。
※ 音声ファイルの形式は、MPG3 形式です。
※ 音声ファイルの登録数は 20 個(合計で 10Mbyte 以内)です。

3　本体への音声ファイルの登録

「登録」をクリックすると、本製品への登録が始まります。

[注　意]

「登録中です」のメッセージ表示中は設定ツールで別操作を行ってはいけません。

4　登録の確認

「音声ファイル一覧」画面に戻り、音声ファイルが登録されたか確認します。
登録されたファイルは「視聴」ボタンで視聴できます

[注　意]

音声ファイルの登録は、空のファイルナンバの若いほうから順に登録されます。ユーザ側で登録するファイルナンバを指定することは出来ません

2-5-1-2 音声ファイルの準備：音声ファイルの視聴

登録した音声ファイルを再生(視聴)するには、本体後面のオーディオ出力ポートに外部オーディオ機器(アンプ内蔵アクティブスピーカやヘッドセットなど)を接続します。

[注　意]

本製品にはアンプやスピーカが内蔵されていません。別途オーディオ機器を用意し接続して利用します。

手順

1 外部オーディオ機器との接続確認･メニュー選択

外部オーディオ機器との接続を確認後、設定画面左ナビメニュー内「音声ファイル登録」―「音声ファイル登録」(上部メニューボタン)をクリックし、「音声ファイル登録」画面(図 2-37 参照)を表示します。

2 音声ファイルの視聴

「音声ファイル一覧」にある「再生／停止 」をクリックすると、それぞれの音声ファイルを再生(視聴)することができます。

2-5-1-3 音声ファイルの準備：音声ファイルのバックアップ

本製品に登録した音声データを PC 等にバックアップします。

手順

1 メニュー選択

設定画面左ナビメニュー内「音声ファイル登録」―「音声ファイルのバックアップ」(上部メニューボタン)(図 2―37 参照)をクリックし、「音声ファイルのバックアップ」画面を表示します。

2 ファイル保存先の指定

「音声データのバックアップ」をクリックすると、ポップアップウィンドウが開きますので、バックアップファイルを「開く」または「保存」を選択してください。

「保存」の場合は、ファイル保存先を指定します。

※ バックアップファイルは圧縮形式で保存されます(gzip 形式)。

※ ポップアップウィンドウ：InternetExplorer9 の場合、画面下側に表示されます。

2-5-1-4 音声ファイルの準備：音声ファイルのリストア

前項で処理したバックアップファイルを本製品にリストアします。

手順

1 メニュー選択

設定画面左ナビメニュー内「音声ファイル登録」―「音声ファイルのリストア」(上部メニューボタ

ン)(図２－37 参照)をクリックし、「音声ファイルのリストア」画面を表示します。

2 リストアの開始

「ファイル名」にバックアップファイル「audio_backup.gz」を指定し、「リストア」ボタンをクリックします。

[注　意]

DN-1500GL 以外で作成したバックアップファイルではリストアできません。

2-5-2 電子メールの準備

警子ちゃんシリーズでは、アクションの一つとして「電子メールによる通知」の機能があります。
この節では、「電子メールの設定」と「電子メールの内容設定」について説明します。

「電子メールの設定」では、既存の電子メールシステムとの連係動作のための情報を設定するのと、通知先を最大５件登録できます。送付先には、グループアカウントや携帯電話のアドレスなども利用できますので、関係者全員や外部での待機要員に通知することも可能です。
また重要な異常通知メッセージをスパムと認知されないために、メールサーバに対する認証方式やアクセスポートの設定なども設定が必要です。
これらの情報は、通常 IT 管理者に確認して入手します。

「電子メールの内容設定」では、送り出される電子メールの「件名」や「本文」を設定します。電子メールの「件名」や「本文」は、規定の文章があり、異常を検知した際の情報を「差し込み処理」した後に電子メールで送り出されます。
電子メールの内容の規定文章は付録を参照します。

2-5-2-1 電子メールの準備：SMTP サーバアクセスの設定

本製品は監視対象の異常などを検知した時に、電子メールによる通知を行うことができます。
本項では、メール送信に必要な SMTP サーバ情報などの設定をします。

手順

1 メニュー選択

画面左ナビメニュー内「電子メール設定」をクリックし、「電子メール設定」画面(図 2-38 参照)を表示します。

図 2-38 電子メール設定画面

2 SMTP サーバアドレス、SMTP ポート番号を指定

SMTP サーバアドレス、およびSMTP サーバの SMTP ポート番号を指定します。

3 認証方式の選択

認証方式のリストから、「認証なし」・「PLAIN」・「LOGIN」・「CRAM-MD5」・「POP before SMTP」を選択し、各認証形式に必要な項目を入力します。

※ 「PLAIN」・「LOGIN」・「CRAM-MD5」の中から選択した場合：

図 2-38 を参照に、④「認証ユーザ名」と⑤「認証パスワード」を入力します

※ 「POP before SMTP」を選択した場合:：

図 2-38 を参照に、⑥「POP before SMTP 認証」の項目を入力します。

4　送信アドレスの設定

図2-38を参照に、⑦送信元となるアドレスを１つ設定します。同様に、⑧送信先のアドレスは最大５件まで登録できます。

送信先に正しくメールが届くか、「テスト送信」ボタンをクリックして、送信先アドレスにテストメールを送信します。

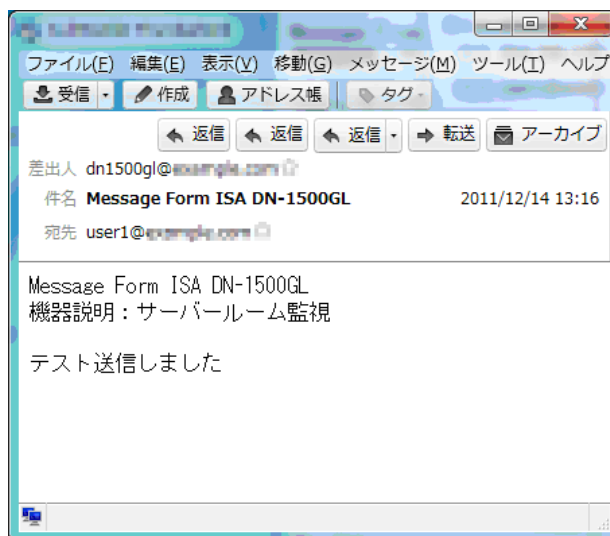



図2-39 テストメール

5　設定内容の反映

画面下の「設定」ボタンをクリックし、設定値に反映させます。

表2-10 SMTPサーバ/認証方式の説明		
項目名	解説	デフォルト値
SMTPサーバアドレス	SMTPサーバのIPアドレス(サーバ名)を入力します。	(空 欄)
SMTPポート	SMTPサーバのSMTPポート番号です。利用環境に合わせて、変更します。	25
認証方式	「認証なし」・「PLAIN」・「LOGIN」・「CRAM-MD5」・「POP before SMTP」から選択します。	(認証なし)
認証ユーザ名	認証方式で「PLAIN」・「LOGIN」・「CRAM-MD5」の中から選択した場合、認証用ユーザ名を入力します。	(空 欄)
認証パスワード	認証方式で「PLAIN」・「LOGIN」・「CRAM-MD5」の中から選択した場合、認証用パスワードを入力します。	(空 欄)

表2-11 POP before SMTP認証の説明		
項目名	解説	デフォルト値
POP3 サーバアドレス	POPサーバのIPアドレス(サーバ名)を入力します。	(空 欄)
POP3 ポート	POPサーバのPOP3ポート番号です。	110
POP3 ログインID	POP サーバ認証のログインIDです。	(空 欄)
POP3 ログインパスワード	POPサーバ認証のログインパスワードです。	(空 欄)

表2-12 送信アドレスの説明		
項目名	解説	デフォルト値
送信元アドレス	送信元となるアドレスを入力します。	(空 欄)
送信先アドレス1~5	送信先のアドレスを入力します。	(空 欄)

2-5-2-2 電子メールの準備：電子メール内容の設定

監視中の異常･回復を検知した時や SNMP トラップを受信した時に、送信するメールの内容を設定します。

件名･本文を 1 組とし、登録できるメールの内容件数は最大 20 件です。

手順

1　メニュー選択

設定画面左ナビメニュー内「メール内容／実行コマンド設定」をクリックし、「メール内容／実行コマンド設定」画面(図 2-40 参照)を表示します。

図 2-40 電子メール内容設定画面

2　メール内容を設定

件名(32 文字以内)、本文(96 文字以内)でメール内容を設定します。

デフォルトメールの文章を差し込み(追加)したい場合、以下の差込文字を「件名」･「本文」に記述します。

「$s」 デフォルトメールのサブジェクト
「$t」 デフォルトメールのタイトル
「$c」 デフォルトメールの本文

「$s」または「$c」を挿入することで、ネットワーク監視の異常と回復をメール内容で判別することができますようになります。

デフォルトメールの各項目は下記になります。

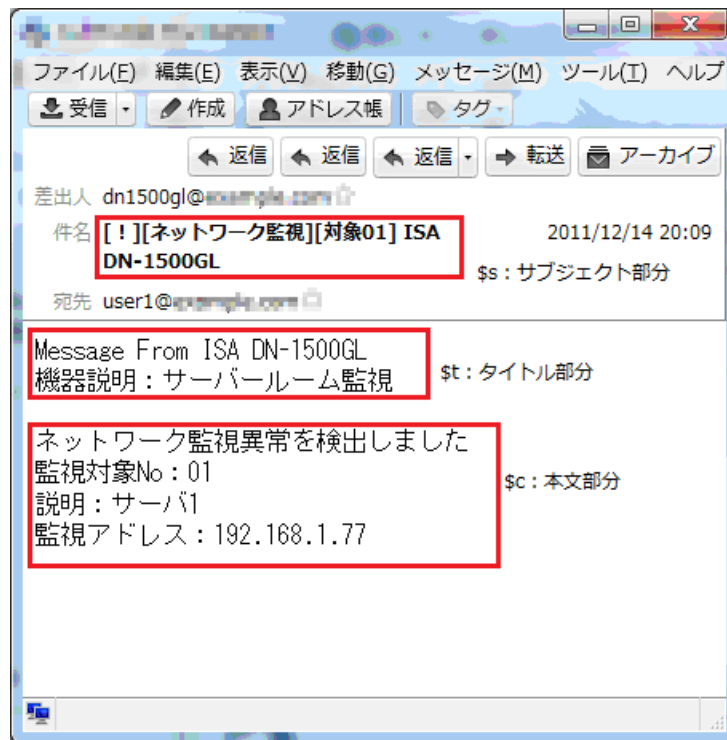



図 2-41 デフォルトメール項目説明

3 設定内容の反映

画面下の「設定」ボタンをクリックし、設定値に反映させます。

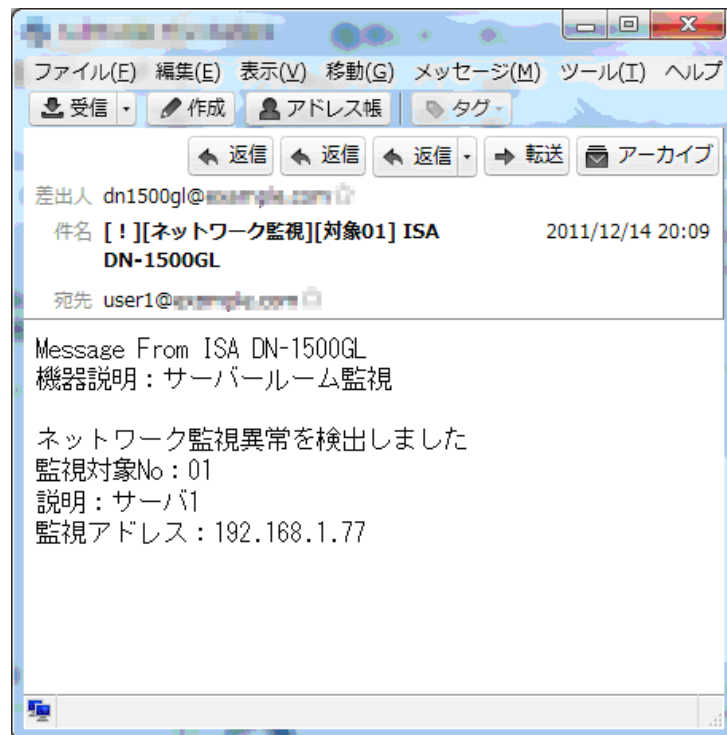



図 2-42 異常検知通知メッセージの例

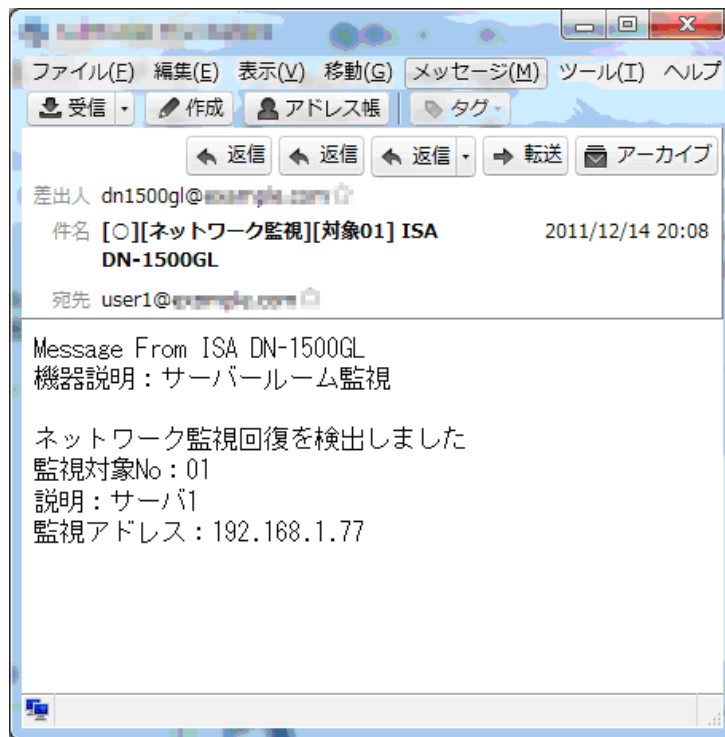



図 2-43 回復検知通知メッセージの例

2-5-2-3 電子メールの準備：イベントログの送信先設定

新規イベントログが 190 レコードを超えたとき、CSV 形式の添付ファイルとして、「イベントログファイル送信先」アドレスに自動送信されます。

※ イベントログは「イベントログファイル送信先アドレス」を設定した場合のみ送信されます。

手順

1 メニュー選択

設定画面左ナビメニュー内「電子メール設定」をクリックし、「電子メール設定」画面を表示します。

2 送信先アドレスの設定

「イベントログファイル送信先アドレス」に送信先アドレスを設定します。

送信アドレス

項目	設定
送信元アドレス	
送信先アドレス-1	テスト送信
送信先アドレス-2	テスト送信
送信先アドレス-3	テスト送信
送信先アドレス-4	テスト送信
送信先アドレス-5	テスト送信
イベントログファイル送信先アドレス	テスト送信

2

設定

図 2-44 イベントログの送信先設定

3　設定内容の反映

画面下の「設定」ボタンをクリックし、設定値に反映させます。

[注　意]

メール未送信のイベントログがさらに 190 レコードを超えた場合は、前回送信したログの次のレコードから 190 レコード分がメール送信されます。

表 2-13 イベントログ送信アドレスの説明		
項目名	解説	デフォルト値
イベントログファイル送信先アドレス	イベントログ送付先のアドレスを入力します。	(空 欄)

2-5-3 SNMP トラップ通知の準備

監視中の異常･回復を検知した時やSNMP トラップを受信した時に事前に登録したSNMP トラップを通知先に送信します。

手順

1　メニュー選択

設定画面左ナビメニュー内「SNMP 設定」をクリックし、「SNMP 設定」画面を表示します。

図 2-45 SNMP トラップ通知の送信先設定画面

2　「アドレス」の入力

通知先の SNMP マネージャの IP アドレス(ホスト名)を入力します。

※ アドレスは、IPv4、IPv6 どちらも入力できます。

※ ホスト名で設定する場合は、DNS サーバの設定が必要です。

3　「コミュニティ名」の入力

それぞれの通知先ごとに「コミュニティ名」を設定します(半角英数字、アンダースコア(“_”)およびハイフン(“-“)で構成された 32 文字以内の文字列)。

4 テスト実行

事前にトラップ送信を確認するには、「テスト実行」ボタンをクリックします。

入力された全てのトラップ通知先にテストトラップを送信します。

5 設定内容の反映

画面下の「設定」ボタンをクリックし、設定値に反映させます。

表 2-14 SNMP トラップ通知先登録の説明		
項目名	解説	デフォルト値
アドレス 1~5	SNMP トラップ通知先の IP アドレス(ホスト名)	(空 欄)
コミュニティ名 1~5	通知先ごとのコミュニティ名	(空 欄)

2-5-4 コマンド実行の準備

監視中の異常･回復を検知した時やSNMP トラップを受信した時に、実行するコマンド(「リモートシェルコマンド」や「snmpset コマンド」など)の内容を設定します。

コマンド種類は 20 件まで登録できます。

手順

1 メニュー選択

設定画面左ナビメニュー内「メール内容／実行コマンド設定」－「実行コマンド設定」(上部メニューボタン)をクリックし、「メール内容／実行コマンド設定」画面(図 2-45 参照)を表示します。

図 2-46 実行コマンド設定画面

2 実行コマンド記述

実行するコマンドを記述します。

[注　意]

コマンドの記述に注意します。

※ ひとつの実行コマンド設定内容として複数のコマンドを登録する場合は、**;(セミコロン)**で区切ります。

※ ひとつの実行コマンド設定内容は、350 文字以内で記述します。

3 設定内容の反映

画面下の「設定」ボタンをクリックし、設定値に反映させます。

2-5-5 TCP ソケット通信の準備

外部の機器やアプリケーションからコマンドを発行して本機を直接制御する場合、rsh コマンド以外に「TCP ソケット通信」を介して実行することが可能です。

複数のポートを設定すると、そのポートそれぞれからコマンドを受け付け、複数の機器やアプリーケーションから本機を共有して利用できます。

「TCP ソケット通信」の設定を行います。

図 2-47 TCP ソケット通信画面

手順

1 メニュー選択

設定画面左ナビメニュー内「TCP ソケット通信設定」をクリックし、「TCP ソケット通信設定」画面(図 2-46 参照)を表示します。

2 通信ポートの指定

ソケット通信に使用する TCP ポートを指定します。ポート数は「開始番号～終了番号」の形式で連続した 10 ポートを指定できます。(デフォルト値 : 60000～60009)

※ポート番号は 1024 以上の番号を指定する必要があります。

3 接続時間の設定

「TCP ソケット通信時間」は、通信がない状態が続いたとき自動的に通信を切断する秒数を入力します。

※1～9999 秒の範囲で指定します。(デフォルト値 : 60 秒)
※「0」入力時は、自動切断されません。

4 行末コードの指定

送受信データの行末コードを指定します。デフォルトは「CR(キャリッジリターン)」です。

※「0A(ゼロ・エイ)」や「0D0A(ゼロ・ディ・ゼロ・エイ)」のように 16 進数を 2 桁単位で 8 桁まで指定が可能です。

5　設定内容の反映

画面下の「設定」ボタンをクリックし、設定値に反映させます。

[TCP ソケット通信で使用できるコマンド]

TCP ソケット通信で使用できるコマンドは、リモートシェル(RSH)コマンドで使用できるコマンドと同じです。詳細は、「2-7-2 コマンドリファレンス」を参照します。

なお、TCP ソケット通信では、アクセスユーザ名の指定およびパスワードの指定はありません。利用にあたっては、十分なシステム考察をお勧めします。

表 2-15 TCP ソケット通信設定の説明

項目名	解説	デフォルト値
通信ポート	ソケット通信に使用する TCP ポートを指定します。 ※ ポート番号は 1024 以上 ※ 10 ポートまで ※ 空欄での設定はできません。	60000　～　60009
ＴＣＰソケット 接続時間（秒）	通信がない状態で自動切断するまでの秒数を指定します。（1～9999 秒） ※「0」入力時は、自動切断されません。 ※ 空欄での設定はできません。	60
行末コード	送受信データの行末コードを指定します。 ※ 16 進数 2 桁単位で 8 桁まで	CR(キャリッジ･リターン)

2-5-6　待機点灯の準備

電源ランプ以外に通常状態を、緑(3 灯モデル)、緑･青･白(5 灯モデル)の 1 灯を、点灯あるいは点滅で常に点灯し、「待機状態」を表します。異常発生時は、待機表示で指定されたランプは消灯し、異常設定で設定されたランプ色(指定されていない場合は消灯)でのアクションが実行され、回復とともに「待機表示」に自動的に戻ります。

「待機点灯」が有効に設定されていると、「表示ランプ」に指定されているランプは「アクション指定」や「コマンドによる制御」は無効になります。

図 2-48 待機点灯設定画面

手順

1 メニュー選択

設定画面左ナビメニュー内｢待機点灯設定｣をクリックし、｢待機点灯｣画面(図 2-47 参照)を表示します。

2 待機点灯の設定

待機時にランプを点灯(点滅)を有効にするには｢待機点灯｣－｢有効｣にチェックを入れます。

3 表示ランプの設定

待機点灯に使用するランプを設定します。

3 灯タイプでは緑ランプのみ、5 灯タイプでは緑･青･白からランプを選択します。

4 表示パターンの指定

待機点灯のランプ表示パターンを｢点灯｣、｢点滅｣、｢高速点滅｣から選択します。

5 設定内容の反映

画面下の｢設定｣ボタンをクリックし、設定値に反映させます。

表 2-16 待機点灯設定の説明

項目名	解説	デフォルト値
待機点灯	「有効」にチェックすると、監視を行います。	無効
表示ランプ	待機時に点灯させるランプを選択します。 3 灯タイプは緑ランプ 5 灯タイプは緑・青・白ランプ より選択します。	緑
表示パターン	「点灯」、「点滅」、「高速点滅」からランプの表示パターンを選択します。	点灯

2-6 外部から制御する

警子ちゃんシリーズでは、システムの運用監視システムを構成するノード監視やネットワーク監視を行うソフトウェア、いわゆるネットワークノード管理ソフト(以下「NNM」と略)と連携して、企業のシステム運用やデータセンターサービスの運用監視に多く利用されています。

NNM の機能を持つソフトウェアは、国内外のソフトウェア会社から販売されています。この多くと警子ちゃんシリーズは連携して運用監視に利用いただいています。

また別の利用方法では、業務アプリケーション、たとえば製造管理、流通管理、顧客管理、電子メールソフト等と連携し、緊急性や異常を分かりやすく伝達する機器として多くの方々にご利用いただいています。

この節では、ネットワークでつながる警子ちゃん 4G を外部から制御する方法を説明します。

たとえば NNM に、異常を検知した際コマンドの実行を記述できる機能があるとき、警子ちゃん 4G の機能をどのように記述するか。また業務アプリケーションからどのようなコマンドを実行すれば警子ちゃん 4G の機能が使えるかを説明します。

外部からのアクセス制御を概念図として次に示します。

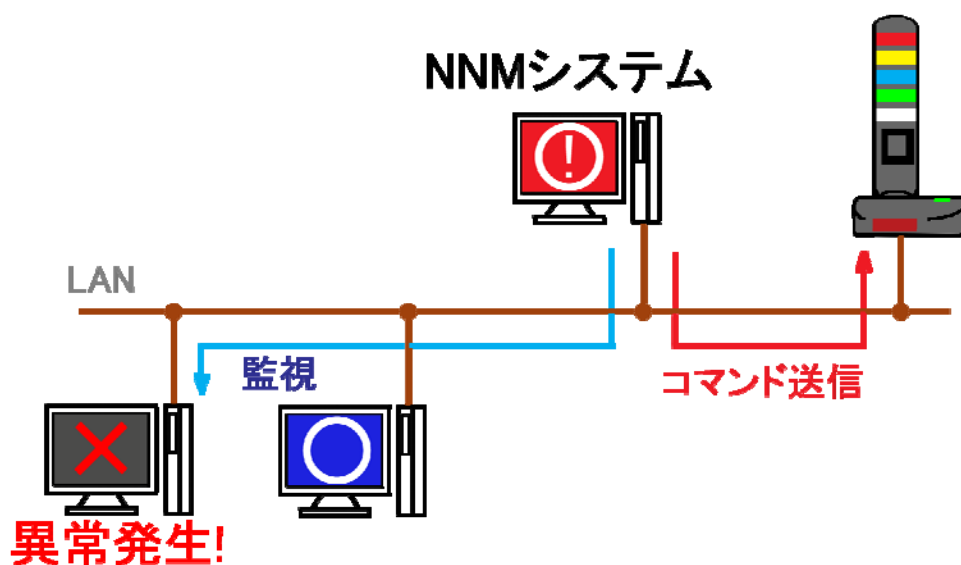



図 2-49 NNM との連係動作概念図

上図では、NNM システムが機器を監視しています。機器で異常が発生すると NNM システムはそれを検知し、判断します。サポート要員が詰める場所に異常発生を通知するため、警子ちゃん 4G に向けてコマンドを発行します。

この図から、ネットワーク上にある警子ちゃんにどのようにアクセスするか、どのようなコマンドを発行するかが重要になります。

この節では、この二点を中心に説明します。

2-6-1 アクセス権の設定

外部から本機に対してコマンドを送る場合、そのアクセスが正当であるかどうかを判断する必要があります。このために「アクセス認証」の設定が事前に必要になります。TCP ソケット通信の場合は「アクセス認証」を必要としません。

2-6-1-1 アクセス権の設定：ユーザ名とパスワードの設定

管理ソフトウェアや業務アプリケーション等と連携させて、リモートシェルを利用し本製品のアラームを動作させる場合は、管理ソフトウェアや業務アプリケーションからのアクセスを許可するための「ユーザ名(アカウント名)」を登録する必要があります。

手順

1 メニュー選択

設定画面左ナビメニュー内「コマンドアクセス設定」をクリックし、「コマンドアクセス設定」画面(図 2-47 参照)を表示します。

図 2-50 コマンドアクセス設定画面

2 ユーザ名の登録

アクセスするユーザ名を「RSH アクセスユーザ名」に登録します。

※ デフォルト値を上書きし、設定します。空欄での設定はできません。

3 パスワードを有効にチェック

「コマンドパスワード」の「有効」にチェックします。

※ パスワードを設定/変更する場合は、「□パスワード変更」へチェックし、「現在のパスワード」と「新しいパスワード」(2 回)を入力してください。

※ パスワードにスペースは使用できません。

4 設定内容の反映

画面下の「設定」ボタンをクリックし、設定値に反映させます。

表2-17 コマンドアクセス設定の説明		
項目名	解説	デフォルト値
ユーザ名 1～5	許可を与える件数分、ユーザ名を入力します。 ※ 半角英数字で 32 文字以内 ※ 大文字･小文字は区別します。 ※ 空欄での設定はできません。	ユーザ 1：root ユーザ 2：Administrator ユーザ 3：SYSTEM ユーザ 4：bin ユーザ 5：root
パスワード機能	「□有効」にチェックを入れます。	(無効)
パスワード	パスワードを入力します。 ※ 半角英数字で 32 文字以内 ※ 大文字･小文字は区別します。 ※ 空欄での設定はできません。	dn1500

[注　意]

1. パスワードを有効から無効に変更する場合
「コマンドパスワード有効」のチェックをはずし、「現在のパスワード」だけを入力し、「設定」ボタンをクリックしてください。
2. パスワードは、Web 設定ツールにログインするためのパスワードと異なるものにします。デフォルト値は、前者が DN1500 で後者が dn1500 です。

2-6-1-2 アクセス権の設定 : SNMP v1/v2c によるアクセスマネージャの設定

本製品に対して外部装置から SNMP でデータ取得/設定(SNMP GET/SET)を行えるように、SNMP アクセスマネージャを設定します。

手順

1 メニュー選択

設定画面左ナビメニュー内「SNMP 設定」―「SNMP アクセス設定(v1/v2c)」(ページ上部)をクリックし、「SNMP　v1/v2c によるアクセスマネージャ」画面(図 2-48 参照)を表示します。

図 2-51 SNMP v1/v2c アクセスマネージャの設定画面

2	マネージャの IP アドレスの入力

アドレス欄に、アクセスマネージャの IP アドレス、またはホスト名を入力します。

※ IPv4、IPv6 どちらも入力できます。

※ ホスト名で設定する場合は、DNS サーバの設定が必要です。

3	アクセス権限の設定

付録の OID リスト「RO(read-only)」、「RW(read-write)」より選択します。

4	コミュニティ名の入力

SNMP のコミュニティ名を入力します(半角英数字、アンダースコア("_")およびハイフン("-")で構成された 32 文字以内の文字列)。入力は任意です。

コミュニティ名により SNMP マネージャとエージェント間の認証を行います

5	設定内容の反映

画面下の「設定」ボタンをクリックし、設定値に反映させます。

表 2-18 SNMP v1/v2c によるアクセスマネージャ設定の説明

項目名	解説	デフォルト値
アドレス	アクセスマネージャの IP アドレス(ホスト名)	(空 欄)
アクセス権	「RO(read-only)」または「RW(read-write)」から選択します。	RO(read-only)
コミュニティ名	SNMP マネージャとエージェント間の認証を行います。	(空 欄)

2-6-1-3 アクセス権の設定 : SNMP v3 によるアクセスマネージャの設定

本製品は SNMP v3 に対応しています。ユーザ毎にセキュリティレベルを指定することができます。認証方式は、User-based Security Mode(USM)です。

手順

1 メニュー選択

設定画面左ナビメニュー内「SNMP 設定」—「SNMP アクセス設定(v3)」(ページ上部)をクリックし、「SNMP v3 によるアクセスマネージャ」画面(図 2-49 参照)を表示します。

図 2-52 SNMP v3 アクセスマネージャの設定画面

2 ユーザ名の設定

アクセスするユーザ名を入力します(半角英数字)。

3 アクセス権限の設定

付録の OID リスト「RO(read-only)」、「RW(read-write)」より選択します。

4 セキュリティレベルの設定

リスト 「非認証·非暗号化」、「認証·非暗号化」、「認証·暗号化」より選択します。

5 認証方式とパスワードの設定 (「認証·非暗号化」と「認証·暗号化」の場合)

ユーザ毎に認証方式とパスワードを設定します。

認証方式は「MD5」と「SHA」のいずれかを設定します。

パスワードは 8~32 文字以内(半角英数字・記号)で設定し、入力します。

6 暗号方式と暗号パスワードの設定 (「認証·暗号化」の場合)

ユーザ毎に暗号方式と暗号パスワードを設定します。

暗号方式は「DES」と「AES」のいずれかを設定します。

暗号パスワードは 8~32 文字以内(半角英数字・記号)で設定し、入力します。

7 設定内容の反映

画面下の「設定」ボタンをクリックし、設定値に反映させます。

表 2-19 SNMPv3 によるアクセスマネージャ設定の説明

項目名	解説	デフォルト値
ユーザ名	アクセスするユーザ名	(空 欄)
アクセス権	「RO(read-only)」または「RW(read-write)」から選択します。	(空 欄)
セキュリティレベル	「非認証･非暗号化」、 「認証･非暗号化」、 「認証･暗号化」から選択します。	(空 欄)
認証方式	使用する認証方式を「MD5」または「SHA」から選択します。	(空 欄)
認証パスワード	認証パスワードです。(半角英数字)8～32 文字以内で入力します。	(空 欄)
暗号方式	使用する暗号方式を「DES」または「AES」から選択します。	(空 欄)
暗号パスワード	暗号パスワードです。(半角英数字)8～32 文字以内で入力します。	(空 欄)

2-6-2 コマンドリファレンス

本製品は、「リモートシェル(RSH)コマンド」と「snmpset コマンド」を用いて外部から制御することができます。

2-6-2-1 リモートシェル(RSH)コマンド

リモートシェルコマンドとその概要を一覧で表 2-18 に記述します。
例は次ページ以降を参照します。
コマンドアクセスを試すときは、事前に前項を参照して登録しておきます。

[注　意]

リモートシェルは通常 UNIX、Windows Server2003、XP、2000、NT より実行可能です。Windows 95、98、VISTA、7、Server2008 では標準でサポートされていません。

[Microsoft Windows 用リモートシェルコマンドについて]

Windows 95、98、VISTA、7、Server2008 で使用可能な Windows 用リモートシェルコマンド、IRSH (ISA Remoteshell)を別途販売しております。デバック機能付きで、LAN プロトコル上の各種情報を表示する事もできます。必要な場合はお問合せください。

詳細は　http://www.isa-j.co.jp/product/softwares/others/IRSH/

表2-20 リモートシェルコマンド一覧 (赤字はDN-1500GLで追加/変更のコマンド)		
コマンド	解　説	READ / WRITE
ACOP	アラーム出力の制御	READ / WRITE
ALOF	アラーム解除	WRITE
CKID	ユーザ名チェック	READ / WRITE
CKIP	ネットワーク監視状態	READ / WRITE
CHST	SNMP トラップ受信状態	READ
HELP	ヘルプ	READ
LGPW	コマンドパスワード	READ / WRITE
PWST	パスワードステータス	READ / WRITE
RDCD	保守契約期限取得	READ
RDCN	保守契約番号取得	READ
RDLP	ランプコード取得	READ
RDMN	モデル名取得	READ
RDPD	製造年月取得	READ
RDSN	シリアル番号取得	READ
RLY1～RLY8	警報出力コントロール（個別）	READ / WRITE
SPOP	音声出力コントロール	READ / WRITE
UTID	ユニット ID	READ
VERN	ファームウェア情報	READ

コマンド入力方法は以下のとおりです。
リモートシェルコマンドの例として、rsh コマンドを使用した場合を記述します。
※ HP-UX では remsh コマンドを使用します。

```
# rsh IP_Address Command [Parameter] [Option] [-p password]
```

※ `IP_Address`部には本製品の IP アドレスを入力します。

[注　意]
全てのコマンドは大文字･小文字を区別しませんが、Parameter は区別するものもあります。
以下のフォーマットに従って入力してください。

① 警報出力コントロール： ACOP

警報装置の出力コントロール及び現在状態の読出し

```
ACOP [(d1) (d2) (d3) (d4) (d5) (d6) (d7) (d8)] [-w <待ち時間(秒)>]
 [-t <継続時間(秒)>] [-p password]
```

モデル	d1	d2	d3	d4	d5	d6	d7	d8
DN-1500GL -x5Lxx	赤	黄	緑	ブザー 連続音 (PPPP…)	ブザー 断続音 (P—P—P—…)	青	白	未使用
DN-1500GL -x3Lxx	赤	黄	緑	ブザー 連続音 (PPPP…)	ブザー 断続音 (P—P—P—…)	未使用	未使用	未使用

内容： 0=OFF(オープン)
1=ON(クローズ)
2=Blink(2 秒周期オープン･クローズ断続)
3=QuickBlink(1 秒周期オープン･クローズ断続)
X=状態保持(X は大文字･小文字を区別しません)

ブザー連続音とブザー断続音を同時に ON または Blink させた場合、ブザー連続音が鳴動し、ブザー断続音は鳴動しません。
｢未使用｣には 0 または X を指定してください。

コントロール時間
-w <待ち時間(秒)> ：指定時間（秒）待って処理を行います。（1～32767 秒, 0 は指定なしと同等）
-t <継続時間(秒)> ：指定時間（秒）後に TurnOff します。（1～32767 秒, 0 は指定なしと同等）
それぞれ省略時は時間コントロールなし。

例１ (5L の場合) 赤を点灯させ、青を点滅にします。他は変更しません。

```
# rsh 192.168.1.211 ACOP 1xxxx2xx [-p password]
```

例２ (3L の場合) 黄を点灯させ、緑を点滅にします。他は変更しません。

```
# rsh 192.168.1.211 ACOP x12xxxxx [-p password]
```

例３ 現在の状態を確認します。

```
# rsh 192.168.1.211 ACOP [-p password]
```

返値： `02010000` (黄色点滅･ブザー連続音鳴動

例４ ブザーを 30 秒間鳴動させます。

```
# rsh 192.168.1.211 ACOP xxx1xxxx -t 30 [-p password]
```

例５ 黄ランプを 10 秒後に 30 秒間点滅させます。

```
# rsh 192.168.1.211 ACOP x2xxxxxx -w 10 -t 30 [-p password]
```

② アラーム解除： ALOF

強制的にランプ･ブザー等を停止させます。

```
ALOF [-p password]
```

例　アラームを停止させます。

```
# rsh 192.168.1.211 ALOF [-p password]
```

③ ユーザ名チェック： CKID

アクセスユーザ名のチェックを有効または無効に設定します。また現在の状態を読み出します。
パラメータ[Enable|Disable]は大文字･小文字を区別します。

CKID [Enable|Disable] [-p password]　【出荷時設定：Enable】

例１　アクセスユーザ名のチェックを無効にします。

```
# rsh 192.168.1.211 CKID Disable
```

root、Administrator またはコマンドアクセス設定ページで登録したユーザ以外でログインしたマシンからもアクセスが可能になります。

④ ネットワーク監視状態： CKIP

ネットワーク監視有効/無効を設定します。また現在の状態を読み出します。

CKIP [(T1)(T2)(T3)(T4)(T5)(T6)(T7)(T8)(T9)(T10)(T11)(T12)(T13)(T14)
(T15)(T16)(T17)(T18)(T19)(T20)] [-p password]

(T1)～(T20)の内容:　E=有効　D=無効　X=状態保持　(大文字小文字を区別しません)

例１　T1 と 3 を有効、T2 を無効、他は変更しません。

```
# rsh 192.168.1.211 CKIP EDEXXXXXXXXXXXXXXXXX
```

例２　現在の状態を確認します。

```
# rsh 192.168.1.211 CKIP
```

返値：　EDDEDDDDDDDDDDDDDDDD　(T1 と T4 のみ監視有効)

※ 有効/無効切り替え処理に時間がかかるため、切り替えは前回設定より約 5 秒以上経過してから行うようにしてください。

⑤ SNMP トラップ受信状態： CKST

SNMP トラップ受信有効/無効の現在の状態を読み出します。

CKST [-p password]

例１　現在の状態を確認します。

```
# rsh 192.168.1.211 CKST
```

返値：　EDDEDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDD
(T1 と T4 のみ受信有効)

⑥ ヘルプ： HELP

コマンドを一覧表示します。またコマンドの内容を表示します。

```
HELP [command] [-p password]
```

例１　コマンドリストの表示

```
# rsh 192.168.1.211 HELP [-p password]
```

例２　コマンド ALOF の説明表示

```
# rsh 192.168.1.211 HELP ALOF [-p password]
```

返値：
```
alof : Alarm OFF
```

⑦ コマンドパスワード： LGPW

パスワードの設定を行います。パスワードは大文字･小文字を区別します。

`LGPW [new-password] [-p password]`　　【出荷時設定：dn1500】

例　出荷時のパスワードを新しいパスワード isa に変更します。

```
# rsh 192.168.1.211 LGPW isa -p dn1500
```

⑧ パスワードステータス： PWST

パスワードを有効または無効に設定します。また現在の状態を読み出します。パラメータ[Enable|Disable]は大文字･小文字を区別します。

`PWST [Enable|Disable] [-p password]`　【出荷時設定： Disable】

例１　パスワードステータスを有効にします。

```
# rsh 192.168.1.211 PWST Enable
```

例２　パスワードステータスを無効にします。

```
# rsh 192.168.1.211 PWST Disable -p password
```

⑨ 保守契約期限取得： RDCD

登録された保守契約期限を読み出します。

```
RDCD [-p password]
```

例
```
# rsh 192.168.1.211 RDCD
```

戻り値：　2017/12/31

⑩ 保守契約番号取得： RDCN

登録された保守契約番号を読み出します。

```
RDCN [-p password]
```

例
```
# rsh 192.168.1.211 RDCN
```

戻り値：　081257

⑪　ランプコード取得：　RDLP

DN-1500 のランプコード(枝番号)を読み出します。

```
RDLP [-p password]
```

戻り値：　5 : DN-1500GL-x5L
　　　　　3 : DN-1500GL-x3L

⑫　モデル名取得：　RDMN

DN-1500GL のモデル名を読み出します。

```
RDMN [-p password]
```

例　DN-1500GL-A5Lxx の場合

```
# rsh 192.168.1.211 RDMN
```

戻り値：　DN-1500GL-A5L

⑬　製造年月取得：　RDPD

DN-1500GL の製造年月を読み出します。戻り値は YYMM 形式で、YY が西暦の下二桁、MM が月です。

```
RDPD [-p password]
```

例　製造年月を読み出します。

```
# rsh 192.168.1.211 RDPD
```

戻り値：　1012　　(2010 年 12 月製造)

⑭　シリアル番号取得：　RDSN

DN-1500xx のシリアル番号を読み出します。

```
RDSN [-p password]
```

例　シリアル番号を読み出します。

```
# rsh 192.168.1.211 RDSN
```

戻り値：　1010120123

⑮ 警報出力コントロール(個別)： RLY1～RLY8

ランプとブザー制御を個々のコマンドで制御し、それぞれ独立して実行します。また個々の現在状態を読出します。

```
RLY<1～8> [TurnOff | TurnOn | Blink] [-w <待ち時間(秒)>] [-t <継続時間(秒)>]
[-p password]
```

RLY 指定(RLY1～RLY8)

モデル	RLY1	RLY2	RLY3	RLY4	RLY5	RLY6	RLY7	RLY8
DN-1500GL -x5Lxx	赤	黄	緑	ブザー 連続音 (PPPP…)	ブザー 断続音 (P―P―P―…)	青	白	未使用
DN-1500GL -x3Lxx	赤	黄	緑	ブザー 連続音 (PPPP…)	ブザー 断続音 (P―P―P―…)	未使用	未使用	未使用

コントロール
TurnOff：OFF（消灯、ブザー停止）
TurnOn：ON（点灯、ブザー鳴動）
Blink：Blink（点滅、ブザー断続鳴動）
文字列は大文字・小文字の区別あり。省略時は現在状態の読出し。

コントロール時間
-w <待ち時間(秒)> ：指定時間（秒）待って処理を行います。（1～32767 秒, 0 は指定なしと同等）
-t <継続時間(秒)> ：指定時間（秒）後に TurnOff します。（1～32767 秒, 0 は指定なしと同等）
それぞれ省略時は時間コントロールなし。

例１　赤ランプを点灯させます。

```
# rsh 192.168.1.211 RLY1 TurnOn [-p password]
```

例２　赤ランプの現在の状態を読み出します。

```
# rsh 192.168.1.211 RLY1 [-p password]
```

戻り値：　TurnOn

例３　ブザーを 30 秒間鳴動させます。

```
# rsh 192.168.1.211 RLY4 TurnOn -t 30 [-p password]
```

例４　黄ランプを 10 秒後に 30 秒間点滅させます。

```
# rsh 192.168.1.211 RLY2 Blink -w 10 -t 30 [-p password]
```

⑯ 音声出力コントロール： SPOP

音声出力コントロール及び現在状態の読出し

SPOP [（d1）（d2）（d3）（d4）（d5）（d6）（d7）] [-p password]

データ 位置	d1	d2	d3	d4	d5	D6	D7	D8
内容	出力状態 0：停止 1：再生	再生する 音声番号 01～20		リピート 再生 0：連続 1：回数指定	リピート再生 回数 01～99		再生前の ブザー出力 0：なし 1：あり	Reserved

※ 現在状態の読み出しは再生状態か停止状態のみ。

※ D7 をセットすると音声再生前に 2 秒間ブザーを鳴動したから音声再生します。

例 1　No1 に登録した音声を連続再生する場合

```
# rsh 192.168.1.211 SPOP 10100000 [-p password]
```

例 2　No9 に登録した音声をブザー出力の後 10 回連続再生する場合

```
# rsh 192.168.1.211 SPOP 10911010 [-p password]
```

例 3　再生中(No9)の音声を停止する場合

```
# rsh 192.168.1.211 SPOP 00000000 [-p password]
```

例 4　現在の状態を取得

```
# rsh 192.168.1.211 SPOP [-p password]
```

返値： 10911010 (再生中)

返値： 00911010 (再生停止)

⑰ ユニット ID： UTID

本製品のユニット ID を呼び出します。ユーザによって変更する事はできません。

UTID [-p password]

例　本製品のユニット ID を呼び出します。

```
# rsh 192.168.1.211 UTID [-p password]
```

返値： 1500

⑱ ファームウェア情報： VERN

本製品のファームウェアバージョンを呼び出します。

VERN [-p password]

例　本製品のバージョンを呼び出します。

```
# rsh 192.168.1.211 VERN [-p password]
```

返値： 14.001.0G

2-6-2-2 snmpset コマンド

本製品の snmp コマンドを使用して、対象機器に値を設定することができます。

制御に利用するコマンドは、「付録 I：SNMP MIB(OID)一覧」を参照します。

書式：

```
snmpset –v <version> -c <community> <ip-address> <oid> <type> <value>
```

<version>：1 または 2c
<community>：コミュニティ名 (必須)
<ip-address>：送信先 IP アドレス
<oid>：オブジェクト ID　(付録：I SNMP MIB(OID)一覧(DN1500GL)を参照)
<type> ： i： INTEGER、s： STRING
<value> 設定する値

使用例：

例１： 外部機器から本機(機種は DN-1500GL、IPv4 アドレスは 192.168.1.10 と仮定)の赤ランプを点灯させるため、snmpset コマンドを利用してコマンドを送る

```
snmpset –v 1 -c public 192.168.1.10 .1.3.6.1.4.1.1333.1.2.6.3.1.0 s 1xxxxxxx
```

public というコミュニティ名で 192.168.1.10 の DN-1500GX にアクセスして、SNMP MIB(OID)一覧にあるランプ制御のコマンド(.1.3~.1.0 の一連の表記)に文字列(s を指定)として 1xxxxxxx の赤点灯の値を、snmpset コマンドで送り出した。

例２： 本機から他の警子ちゃん(機種は DN-1500GL、IPv6 アドレスは[fd00:d0:a8:1::10]と仮定)の赤ランプを点灯させるため、snmpset コマンドを利用してコマンドを送る

```
snmpset –v 1 -c public upd6:[fd00:d0:a8:1::10] .1.3.6.1.4.1.1333.1.2.6.3.1.0
s 1xxxxxxx
```

public というコミュニティ名で[fd00:d0:a8:1::10]の DN-1500GL にアクセスして、SNMP MIB(OID)一覧にあるランプ制御のコマンド(.1.3~.1.0 の一連の表記)に文字列(s を指定)として 1xxxxxxx の赤点灯の値を、snmpset コマンドで送り出した。

注意事項

1. ISA 製品宛に snmpset コマンドを実行する場合、受信側装置の「SNMP アクセス設定」に送信元の IP アドレス、コミュニティ名、read/write 許可を設定します。
2. PC やサーバ等宛てに snmpset コマンドを送信する場合、受信側に snmpset コマンドを受信するためのサービス(snmpd 等)が動作している必要があります。
また、通信経路上や rsh コマンドを受ける PC やサーバにファイアウォールを立てている場合、161 番ポートでの snmp 通信を許可する必要があります。

2-6-2-3 TCP ソケット通信でのコマンド制御

本機を TCP ソケット通信に対応するために、事前に準備します(「2-5-5 TCP ソケット通信の準備」参照)。次に TCP ソケット通信を本機と他の装置との間で確立させます。その後、アプリケーションや既存のソフトウェアから本機に対してコマンドを送り出します。WRITE 系、READ 系コマンドともに戻り値があります。

コマンドは、「2-6-2-1 リモートシェル(RSH)コマンド」がそのまま使えます。

TCP ソケット通信は、コネクションが確立されると送り手と受け手の間で個別に情報のやりとりができます。またイベントログに記録されます。

たとえば、「警報出力コントロール：ACOP」を外部の機器から送り出し、赤を点灯させ青を点滅させる場合は次の様になります(5 灯モデルで、他のランプは変更せず)。

```
ACOP 1xxxx2xx
```

※ 各コマンドには、オプションでパスワードの設定が可能ですが、TCP ソケット通信では不要です。(付けるとエラーになります)

上記例の様に ACOP を WRITE 系コマンドとして正常に実行されると、「2-5-5 TCP ソケット通信の準備」で設定した「行末コード」が返されます (READ 系コマンドは、戻り値と行末コード)。正常に実行されない場合は、以下のエラーコード(ERxx)と行末コードが返され、イベントログに記録されます。

“ER01”: 無効なコマンド、”ER02”: 行末コードが異なる、
“ER03”: コマンド引数の間違い、”ER04”: コマンド実行失敗

2-7 確認する

ここでは、警子ちゃん 4G が監視を続ける中で、アラームが動作したり電子メールで通知してきたとき、その詳細を確認する方法を説明します。

確認は、警子ちゃん 4G の「Web 設定ツール」を介して行います。従って、本体に設定されている「IP アドレス」を事前に準備しておく必要があります。

2-7-1 監視対象の状況確認

「ネットワーク死活監視」対象の状況確認は、本体にアクセスした最初のページ、「Web 設定ツール」画面のトップ画面(「モニタ画面」ともいう)に表示されています。

状況は画面の「オートリフレッシュ」ごとに更新して表示されます。

手順

1 IP アドレスを入力します

Web ブラウザを起動し、アドレスに警子ちゃん 4G に設定されている IP アドレスを入力し(図 2-50 参照)、[Enter]キーを押します。
するとモニタ画面(図 2-51 参照)が表示されます。

図 2-53 Web ブラウザに IP アドレスを入力

図 2-54 モニタ画面

2 モニタ画面から確認します

モニタ画面には、問い合わせやサービス確認のための「本体情報」、「現在時刻」、「本体内部温度」、「機器説明」、およびネットワーク監視対象で登録された機器の「監視対象」名称、「監視」の有無、「説明」、「状態」の正常/異常、RTT の「監視」有無、「閾値」および「平均値」が表示されます。

各々の項目説明は、表 2-21 を参照します。

図 2-55 対象機器の監視が有効で正常なときの表示例

図 2-56 対象機器の監視が有効で異常を検知したときの表示例

<table>
<tr><th colspan="3">表 2-21 モニタ画面表示内容の説明</th></tr>
<tr><th colspan="2">項目名</th><th>解説</th><th>デフォルト値</th></tr>
<tr><td colspan="2">現在時刻</td><td>日付と現在の時刻が表示されます。
表示書式は、年月日(西暦)(yyyy/mm/dd)、曜日(w)、時間(hh:mm JST)になります。
時間の更新は「オートリフレッシュ」ごとになります。</td><td>―</td></tr>
<tr><td colspan="2">本体内部温度</td><td>本製筐体に内蔵されている温度センサが計測している温度を表します。
この温度が 70℃を超えると、設定された通知先アドレスに内部温度異常のトラップ(enterprise：「.1.3.6.1.4.1.1333.1.2.6.4.3」、generic-trap：「6」、specific trap：「4」)が送信されます。</td><td>―</td></tr>
<tr><td colspan="2">機器説明</td><td>「本体情報」で設定された「機器説明」が表示されます。</td><td>(空 欄)</td></tr>
<tr><td colspan="2">監視対象</td><td>現在ネットワーク死活監視(Ping 監視)が設定されているネットワーク･デバイスの IP アドレスまたはホスト名が表示されます。</td><td>(空 欄)</td></tr>
<tr><td colspan="2">監視</td><td>監視対象の監視の有効または無効が表示されます。
※ 監視対象毎に監視の 有効 / 無効 が設定できます。</td><td>無効</td></tr>
<tr><td colspan="2">説明</td><td>監視対象の説明です。</td><td>(空 欄)</td></tr>
<tr><td colspan="2">状態</td><td>監視対象の状態です。
【状態表示に関して】<table><tr><td>正常（緑）</td><td>正常</td><td>正常時</td></tr><tr><td>警告（赤）</td><td>警告</td><td>監視対象の異常を検出し、本製品がアラーム ON の状態</td></tr><tr><td>警告（黄）</td><td>警告</td><td>監視対象の異常を検出し、本製品が強制アラーム OFF（アラーム解除）されている状態</td></tr></table></td><td>(空 欄)</td></tr>
<tr><td colspan="2">RTT</td><td>ラウンドトリップタイム
「送信回数」で設定した Ping 送信回数分のラウンドトリップ時間の平均の閾値を設定し監視します。</td><td>―</td></tr>
<tr><td rowspan="3">RTT</td><td>監視</td><td>RTT の監視の 有効 または 無効 が表示されます。</td><td>無効</td></tr>
<tr><td>閾値</td><td>「平均 RTT 閾値」で設定された Ping 送信回数分のラウンドトリップ時間の平均の閾値が表示されます。</td><td>1000ms</td></tr>
<tr><td>平均値</td><td>Ping 送信回数分のラウンドトリップ時間の平均値が表示されます。この値が左の「閾値」を超えると、異常と判定され「状態」が 警告 となります。</td><td>0ms</td></tr>
</table>

2-7-2 イベントログの確認

監視対象の異常の発生、回復のほかに、コマンド受信などのイベントログを「タイムスタンプ」と共に内蔵のフラッシュメモリへ保存します。
ここでは、「Web 設定ツール」画面から記録されたイベントログを確認します。

事前に「イベントログの送信設定(2-5-2-3 参照)」を行うことで、イベントが 190 を超えたところで指定されたアドレスに CSV 形式ファイルを添付して送り出します。

イベントログとして扱われる内容項目は付録を参照します。

イベントログの最大記録件数は 200 件です。200 件を超えて新しいイベントが発生すると、一番古いイベントログが消え、新しいイベントログが記録されます。
本体内に記録されているイベントログは、「イベントログクリア」以外消去する方法はありません。

手順

1 Web 管理ツールにログインします
Web ブラウザに警子ちゃん 4G の IP アドレスを入力し、Web 管理ツール画面を表示させます。次にログインし設定画面を表示させます。

2 メニューの選択
左ナビメニューから「管理ツール」の「イベントログ」をクリックします。
イベントログ画面が表示されます。
各ログは、「年月日」と「時刻」をタイムスタンプとして「発生イベント」と一緒に記録されます。

管理ツール > イベントログ

イベントログ

No.	年月日	時刻	発生イベント
1	2011-12-19	09:32:58	デバイス 1 (192.168.1.5) 警報 On
2	2011-12-17	17:39:47	ツールによるアラーム解除
3	2011-12-17	16:05:01	ツールによるアラーム解除
4	2011-12-17	16:00:16	ツールによるアラーム解除
5	2011-12-17	11:21:47	スイッチによるアラーム解除
6	2011-12-17	11:21:34	デバイス 1 (192.168.1.5) 警報 On

図 2-57 イベントログ画面

3 確認し終わったら
イベントログのリストは、通常の Web 画面同様にコピーアンドペーストができます。
確認後はそのままログアウトするか、次の手順で消去あるいは記録できます。

4 イベントログの消去/記録
イベントログ画面の下部には、「イベントログクリア」と「イベントログ保存(CSV)」のボタンがあります。

「イベントログクリア」を押すと、今画面にリストされているイベントログがすべて消去されます。設置場所などが変わったり、試験運用から本番運用に変わるときなどに利用します。
「イベントログ保存(CSV)」を押すと、画面にあるイベントログを CSV ファイル形式で PC 等に取り込むことができます。

2-8 メンテナンスする

ここでは、本体を他の環境に移設するような場合に必要となる、ファームウェアの更新、初期化、設定内容のバックアップ、リストア等について理解を深めます。

2-8-1 ファームウェアの更新

本製品の基本的な制御を行うために機器に組み込まれたソフトウェアを「ファームウェア」といいます。更新は有線 LAN を使って行います。

(最新バージョン含め)ファームウェアを以下の手順の説明で記述したサイトよりダウンロード後、本製品(警子ちゃん)へアップデートし、利用します。

※ 各バージョンの詳細を確認の上、ファームウェアのダウンロードを行います。

無線 LAN 環境下でのファームウェア更新はお勧めしません
無線 LAN 環境下で本機を利用されていても、ファームウェア更新の際には有線 LAN 環境で実施することを強くお勧めします。これは有線 LAN 環境での通信が無線 LAN より確実なためです。ファームウェア更新が中断すると故障の原因になります。

手順

1 ファームウェアのダウンロード
下記のダウンロードサイトより、該当ファームウェアを PC 等に保存します。

ファームウェア･ダウンロードサイト
ユーザ登録完了後 URL をメールでご案内します

図 2-58 ファームウェアダウンロードサイトにアクセス

2 ログインとメニュー選択
本体にログインにします。
設定画面左ナビメニュー内「ファームウェアアップデート」をクリックし､「ファームウェアアップデート」画面(図 2-58 参照)を表示します。

図 2-59 ファームウェアアップデート画面

3 ファームウェアファイルの選択

前述の 1 でダウンロードしたファイルの名前やディレクトリなどを確認しておきます。

ファイルの指定：

「参照」をクリックし、 1 でダウンロードしたファームウェアファイルを選択します。

「実行」ボタンをクリックします。

※ 誤ったファイルを選択し実行した場合：
「正しいアップデートファイルを指定してください」というメッセージが出ます。
正しいファイルを選択し直し実行します。

4 ファームウェアのアップデート

「ファームウェアのアップデートを実行しますか」とメッセージが表示されますので、「OK」をクリックします。

アップデートが開始されると「アップデート中です…」と表示されます。

※ アップデート中は、他操作を行ってはいけません。

5 再起動(自動)

アップデート完了後、(本製品は)自動的に再起動されます。再起動が開始されると「再起動中です」と表示されます。

再起動中の注意事項

再起動完了まで、2～3 分かかります。

再起動中は操作ができませんので、再起動完了まで、お待ちください。

---

6 再起動完了

再起動完了後、[ファームウェアアップデート]トップ画面 1 へ戻ります。

表 2-22 ファームウェア更新に関する注意事項

項目名	解　　説
ダウンロードサイト	※ ダウンロードサイトはユーザ登録を頂いたお客様のみにメールにてご案内させて頂いております。 ※ 無断でのリンク等はお断り致します。
追加項目について	最新のファームウェアで追加された項目には工場出荷時の値が設定されています。
作業上の注意事項	以下の作業中は、本製品の電源を切らないでください。 ※ ファイルのフラッシュ(本体内蔵フラッシュメモリへの書き込み)中 ※ ファイルのアップロード(PC 等から本体にファイルを転送)中 ※ ファイルのアップロード中は本製品のネットワークケーブルも取り外さないでください。 →作業内容が正常に終了せず、以降の動作に支障をきたす恐れがあります。

14.150.0G 以前のファームウェアよりアップデートを行う場合
SNMP トラップ監視の設定を設定しなおす必要があります。
『付録 L：14.150.0G 以前のファームウェアをお使いの場合』を参照ください。

2-8-2 本体の再起動

「監視対象などがハングアップ状態」や「本製品の動作が不安定」の際は、本製品を再起動します。
再起動を行っても、設定情報の再入力する必要ありません。

手順

1 メニュー選択

設定画面左ナビメニュー内「再起動」をクリックし、「再起動」画面(図 2-59 参照)を表示します。

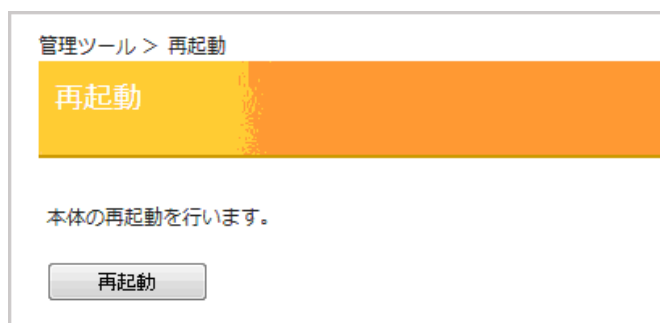



図 2-60 再起動画面

2 再起動

「再起動」をクリックすると、「DN-1500 を再起動します。」とメッセージが表示されますので、「OK」をクリックします。
再起動が開始されると「再起動中です…」と表示されます。

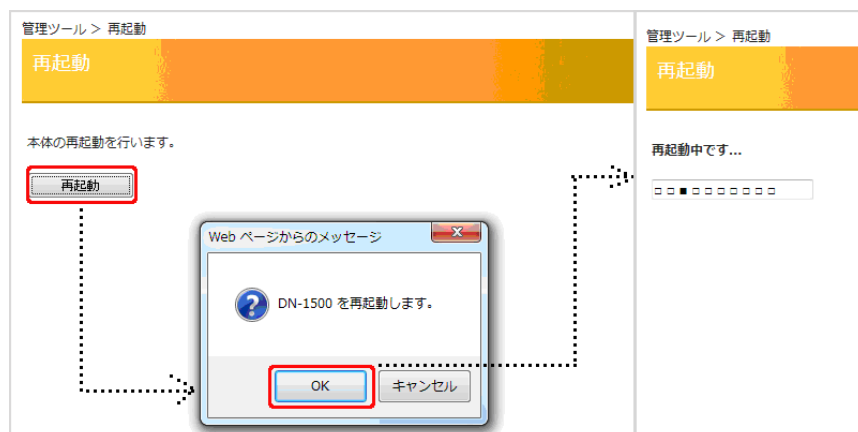



図 2-61 再起動→再起動開始メッセージ

再起動中の注意事項
※ 再起動完了まで、2～3 分かかります。
※ 再起動中は操作ができませんので、再起動完了まで、お待ちください。

2-8-3 初期化(工場出荷時の設定に戻す)

本製品の設定を初期化します(工場出荷時の状態に戻します)。
「LAN 設定」ページの内容は変更されず、「管理ユーザ設定」は初期化されません。

手順

1 メニュー選択

設定画面左ナビメニュー内「設定初期化」をクリックし、「設定初期化」画面(図 2-61 参照)を表示します。

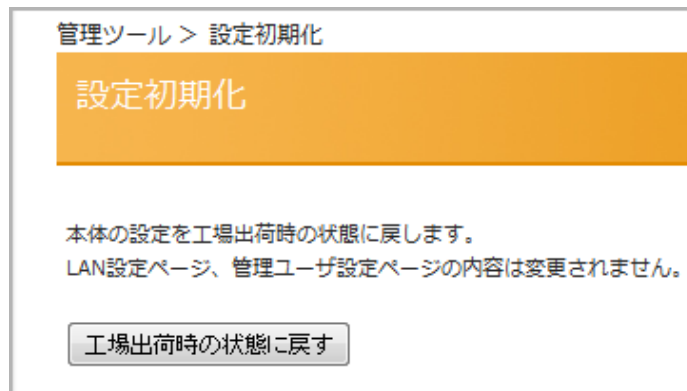



図 2-62 設定初期化画面

2 設定初期化

「工場出荷時の状態に戻す」をクリックすると、「工場出荷時の設定に戻してもよろしいですか？」とメッセージが表示されますので、「OK」をクリックします(図 2-62 参照)。
設定初期化が開始されると「設定初期化後、再起動します。」と表示されます。

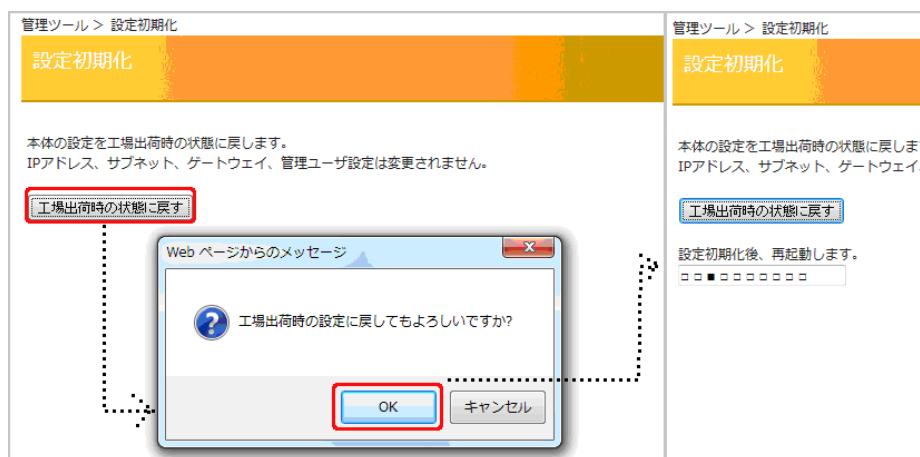



図 2-63 設定初期化、操作の流れ

3 再起動(自動)

設定初期化完了後、(本製品は)自動的に再起動されます。
再起動が開始されると「再起動中です…」と表示されます。

再起動中の注意事項

※ 再起動完了まで、2～3 分かかります。

※ 再起動中は操作ができませんので、再起動完了まで、お待ちください。

図 2-64 再起動中画面

4 設定初期化完了
再起動完了後、[設定初期化]トップ画面 1 へ戻ります。

2-8-4 設定データのバックアップ

本製品に設定したデータをバックアップします。
「設定変更後」は、本処理を行うことをお奨めします。

手順

1 メニュー選択
設定画面左ナビメニュー内「設定データのバックアップ/リストア」をクリックし、「設定データのバックアップ/リストア」画面(図 2-64 参照)を表示します。

図 2-65 設定データのバックアップ/リストア画面(バックアップ)

2 設定データのバックアップ
「バックアップ」をクリックします。
「ファイルを保存しますか？」という内容のポップアップウィンドウが表示されますので、任意のフォルダにファイルを保存します。

バックアップファイルのデフォルト名は「backup.gz」です。

2-8-5 設定データのリストア

設定データのバックアップファイル「backup.bz」を本製品にリストアします。
この機能を使うと、複数台の警子ちゃん導入時に同じ仕様の設定データをストアすることができ、作業効率が改善されます。

手順

1 メニュー選択
設定画面左ナビメニュー内「設定データのバックアップ/リストア」をクリックし、「設定データのバックアップ/リストア」画面を表示します。

図 2-66 設定データのバックアップ/リストア画面(リストア)

2 バックアップファイルの指定
「設定データリストア」－「ファイル名」「参照」をクリックし、前項で「バックアップ」したファイル「backup.gz」を選択します。
※ 「リストア」ボタンをクリックします。
リストアする選択項目が表示されますので、リストアする項目にチェックを入れます。
※ファイル名を変更した場合は、「backup.gz」へ変更後、リストア作業を行ってください。

3 項目の指定
次の画面から、リストアしたい項目にチェックを入れ、「リストア」ボタンをクリックします。

※ IP アドレス、サブネットマスク、ゲートウェイ、管理ユーザ設定はリストアできません。

[注　意]
DN-1500GL 以外で作成したバックアップファイルではリストアできません。

14.150.0G 以前のファームウェアよりリストアを行う場合
SNMP トラップ監視の設定を設定しなおす必要があります。
『付録 L：14.150.0G 以前のファームウェアお使いの場合』を参照ください。

表 **2-23** 設定データリストア項目の説明	
項目名	解　説
本体情報	装置説明、オートリフレッシュ、オートログアウト
無線 LAN アクセス	ESSID、暗号化モード、暗号強度、指定方式、WEP キー、WPA PSK キー、アクティベーションキー
NTP サーバによる時刻設定	NTP 有無、NTP アドレス、時間確認間隔、タイムゾーン
電子メール設定	SMTP サーバドレス、SMTP ポート番号、認証方式、認証ユーザ名、認証パスワード、送信元アドレス、送信先アドレス 1~5、イベントログ先アドレス
SNMP 設定	SNMP トラップ： 通知先アドレス、コミュニティ名 SNMP v1/v2c： マネージャアドレス、アクセス権、コミュニティ名 SNMP v3： ユーザ名、アクセス権、セキュリティレベル、認証方式、認証パスワード、暗号化方式、暗号化パスワード
コマンドアクセス設定	RSH： ユーザ名 1~5、コマンドパスワード、パスワード、ユーザ ID チェック
メール内容／実行コマンド設定	件名、本文、コマンド
TCP ソケット通信設定	通信ポート、TCP ソケット持続時間、行末コード
待機点灯設定	待機点灯、表示ランプ、表示パターン
ネットワーク監視設定	ネットワーク監視設定は監視機能の「ネットワーク監視設定」と「ネットワーク監視アクション一覧/設定」の設定内容をバックアップします。
SNMP トラップ監視設定	SNMP トラップ監視設定は監視機能の「SNMP トラップ監視設定」と「SNMP トラップ監視アクション一覧/設定」の設定内容をバックアップします。
アラーム解除設定	解除方法、解除モード、アラームボタン監視の有無、アラームボタン監視アクション設定項目
イベントログ	日付と時間、タイムゾーン、イベントログ
端末状態アクション設定 (機器連携用)	機器連携についての別紙連携マニュアルを参照します。

2-8-6 設定データのエクスポート

設定データを個別に CSV 形式のファイルでエクスポートします。

手順

1 メニュー選択

設定画面左ナビメニュー内「設定データのバックアップ/リストア」をクリックし、「設定データのバックアップ/リストア」画面を表示します。

エクスポートしたファイルの内容は変更して、インポートすることができます。

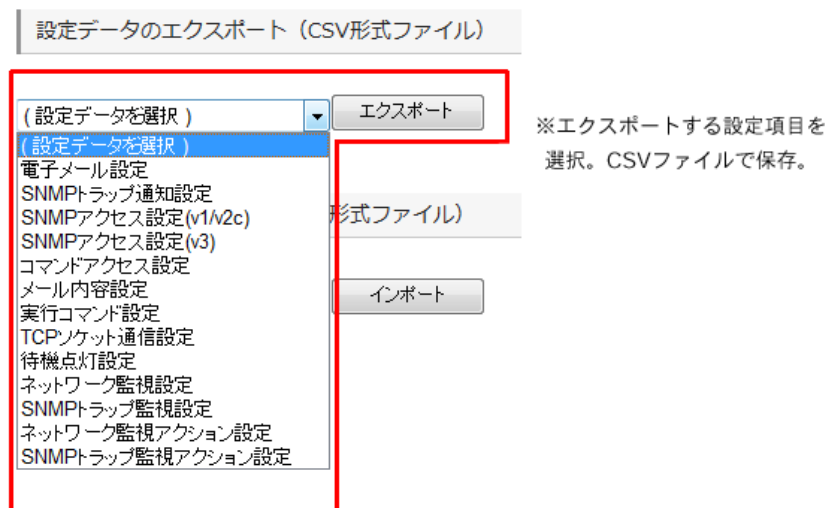



図 2-67 設定データのバックアップ/リストア画面(設定データのエクスポート)

2 設定データの指定

エクスポートしたい「設定データ」を選択し、「エクスポート」ボタンをクリックします。

[注　意]

エクスポートした CSV ファイルを EXCEL(エクセル)で開く際は、表示形式を「文字列」にするよう、注意してください。

数字のみで「0」で始まるデータは、数値形式で開くと最初の「0」が省略してしまい、認識と違うデータがインポートされる場合があります。

例) エクスポートしたデータ「0123456789」

数値形式で開くと>>>「123456789」

2-8-7 設定データのインポート

設定データを個別に CSV 形式のファイルでインポートします。

手順

1 メニュー選択

設定画面左ナビメニュー内「設定データのバックアップ/リストア」をクリックし、「設定データのバックアップ/リストア」画面を表示します。

設定データバックアップ

バックアップするにはボタンを押下してください。

バックアップ

設定データリストア

参照... リストア

設定データのエクスポート（CSV形式ファイル）

（設定データを選択） エクスポート

設定データのインポート（CSV形式ファイル）

参照... インポート ※CSVファイルを選択

図 2-68 設定データのバックアップ/リストア画面(設定データのインポート)

2 インポートファイルの指定

「設定データインポート」－「ファイル名」「参照」をクリックし、前項で「エクスポート」した CSV ファイルを選択します。

※ 「インポート」ボタンをクリックします。

[注　意]

DN-1500GL 以外で作成した CSV ファイルではインポートできません。

表 2-24 設定データエクスポート/インポート項目の説明	
項目名	解　　説
電子メール設定 (mail.csv)	「詳細設定」－「電子メール設定」の内容をエクスポート/インポートします。
SNMP トラップ通知設定 (trap.csv)	「詳細設定」－「SNMP 設定」－「SNMP トラップ通知設定」の内容をエクスポート/インポートします。
SNMP アクセス設定(v1/v2c) (snmpv12c.csv)	「詳細設定」－「SNMP 設定」－「SNMP アクセス設定(v1/v2c)」の内容をエクスポート/インポートします。
SNMP アクセス設定(v3) (snmpv3.csv)	「詳細設定」－「SNMP 設定」－「SNMP アクセス設定(v3)」の内容をエクスポート/インポートします。
コマンドアクセス設定 (rsh.csv)	「詳細設定」－「コマンドアクセス設定」の内容をエクスポート/インポートします。
メール内容設定 (mail_content.csv)	「詳細設定」－「メール内容設定」の内容をエクスポート/インポートします。
実行コマンド設定 (exec_cmd.csv)	「詳細設定」－「実行コマンド設定」の内容をエクスポート/インポートします。
TCP ソケット通信設定 (tcp_socket.csv)	「詳細設定」－「TCP ソケット通信」の内容をエクスポート/インポートします。
待機点灯設定 (standby_lamp.csv)	「詳細設定」－「待機点灯設定」の内容をエクスポート/インポートします。
ネットワーク監視設定 (ping_mon.csv)	「監視設定」－「ネットワーク監視設定」－「ネットワーク監視」の内容をエクスポート/インポートします。
SNMP トラップ監視設定 (trap_mon.csv)	「監視設定」－「SNMP トラップ監視設定」－「SNMP トラップ監視」の内容をエクスポート/インポートします。

表 2-24 設定データエクスポート/インポート項目の説明(続き)	
項目名	解　説
ネットワーク監視アクション設定 (ping_act.csv)	「監視設定」―「アクション設定」―「ネットワーク監視」の内容をエクスポート/インポートします。
SNMP トラップ監視アクション設定 (trap_act.csv)	「監視設定」―「アクション設定」―「SNMP トラップ監視」の内容をエクスポート/インポートします。
端末状態アクション設定 (機器連携用)	機器連携についての別紙連携マニュアルを参照します。
※（）内はエクスポートした際のファイル名です。変更したファイル名もインポートは可能です。	

2-8-8 メンテナンス時などでのアクションの一時停止

監視対象毎に監視の 有効 または 無効 を設定できるので、システムメンテナンス時などの際に本製品の監視を一時的に停止させ、アラームが動作しないようにすることができます。

手順

1 メニュー選択

設定画面左ナビメニュー内「ネットワーク監視設定」、「SNMP 監視設定」または「アラーム解除設定」画面(図 2-66 参照)を表示します。

図 2-69 ネットワーク監視設定、SMTP 監視設定、アラーム解除設定での監視設定

2 監視の一時停止

監視を一時停止したい対象の「有効」チェックをはずします。

3 設定内容の反映

画面下の「設定」ボタンをクリックし、設定値に反映させます。

[注　意]

メンテナンス終了後、監視を再開するには再度「有効」にチェックを入れて、設定を反映してください。

付録 A: トラブルシューティング

トラブル発生時、以下をご参照ください。

<table>
<tr><th>トラブル状態</th><th>推定原因と処置</th></tr>
<tr><td>壊れたかなと思ったら</td><td>再起動させるため、一度電源を抜いてください。再度電源を投入し状態が改善されるか確認します。</td></tr>
<tr><td>IP アドレスを忘れてしまった
(IP アドレスを初期化したい)</td><td>IP アドレスを初期化する必要があります。
手順
<table>
<tr><td>1</td><td>本製品の電源を一度切り、再起動させます。
(本体背面の AC アダプタコネクタを抜き挿ししてください)</td></tr>
<tr><td>2</td><td>本体起動時に「赤・緑・黄」とランプが点灯します。
(約 0.5 秒間隔で順次点灯後、順次消灯します)</td></tr>
<tr><td>3</td><td>赤/黄/緑いずれかのランプ点灯中にアラームストップボタンを押し、約 15 秒間長押しします。
※ボタン押下時にランプは全て消灯します。</td></tr>
<tr><td>4</td><td>約 15 秒後に赤ランプ点灯後、順に黄点灯→緑点灯→全ランプ消灯し、初期化を実行します。</td></tr>
<tr><td>5</td><td>工場出荷時 IP アドレス : 192.168.1.1 で設定ツールにアクセスし、IP アドレスを変更してください。</td></tr>
</table>
【初期化する項目と工場出荷時設定値】
※下記以外の項目は変更されません。
<table>
<tr><th></th><th>有線 LAN IPv4</th><th>無線 LAN IPv4</th></tr>
<tr><td>アドレス</td><td>192.168.1.1</td><td>空　欄</td></tr>
<tr><td>サブネットマスク</td><td>255.255.255.0</td><td>255.255.255.0</td></tr>
<tr><td>ゲートウェイアドレス</td><td>192.168.1.254</td><td>空　欄</td></tr>
</table></td></tr>
<tr><td>電源投入後ランプが全点灯し起動しない</td><td>暫く電源 OFF の後に通電を行うと、RTC のバックアップコンデンサ充電のためにすぐに起動できない場合があり、全ランプが点灯します。
10 分ほど通電状態とした後に電源を OFF→ON してください。</td></tr>
<tr><td>WEB でアクセスできない
ping が通らない</td><td>LAN ケーブルが挿入されているか確認します。
電源投入後、3 分以上経過していますか？本体が立ち上がるまで 2~3 分かかります。この間は正しい動作が行えません。
一度 IP アドレスを初期化して、正しい値に再度設定し直します。</td></tr>
<tr><td>ping は通るが、WEB でアクセスできない</td><td>WEB ブラウザがプロキシサーバを参照していませんか？
プロキシサーバが本製品と接続できる設定がされていない場合、WEB 画面は見えません。
WEB ブラウザの「ツール＞インターネットオプション＞接続＞LAN の設定＞プロキシサーバ」のチェックボックスを外し、本製品の WEB 画面が参照できるか確認してください。
見える場合、ネットワーク管理者とご相談ください。</td></tr>
</table>

トラブル状態	推定原因と処置
「既に他のユーザがログインしています。」というメッセージが表示され、設定ツールにログインできない	ブラウザのアドレス部に「http://192.168.1.1/ logout」と入力し実行してください。(192.168.1.1 部分は本製品の IP アドレスを入力してください) ※強制ログアウトさせる際は、他のユーザがログインしていないか必ず確認してください。
リモートシェルのコマンドパスワードを忘れてしまった	本製品の設定を工場出荷時の状態に戻す必要があります。 処理を実行する前に「設定データのバックアップ」を行えば、コマンドアクセス設定だけを工場出荷時の状態に戻す事ができます。 「設定データのバックアップ」→「設定初期化」→「設定データのリストア」でコマンドアクセス設定以外を選択します。
WEB ツールの管理ユーザ名･パスワードを忘れてしまった	ユーザ名･パスワードのみ初期化する必要があります。 本製品の型番とシリアル番号をお控えの上、弊社カスタマーサポートセンター(TEL：03-3208-1243)にご連絡ください
ALARM STOP ボタンを押しても、ランプとブザーのテスト実行ができない	本製品が異常を検知している間、テストは実行されません。また本製品起動中(電源投入から 2～3 分程)も実行されません。
異常ではないのに、アラームが頻繁に発生している	ネットワークが不安定な状態なのかもしれません。 ユニット設定ページでモニタ間隔、応答確認回数を増やしてみます。
リモートシェルでアクセスできない	工場出荷時の状態でアクセス可能なログインユーザは root、Administrator、SYSTEM、bin です。 コマンドアクセス設定ページでユーザを登録いただくか、-l オプションで root、Administrator、SYSTEM、bin をご指定ください。 例) `rsh 192.168.1.1 -l root ACOP` 登録後もアクセスできない場合は OS やウィルスソフトのファイアウォールの設定をご確認ください。 WindowsXP SP2 以降については以下詳細をご参照ください。 詳細： http://www.isa-j.co.jp/support/accept/
Windows からの実行で、リモートシェルが完了しない、プロンプトが戻ってこない	-n オプションを追加してお試しください。 例) `rsh 192.168.1.1 -n ACOP`
コマンドプロンプトからはリモートシェルでアクセスできるが、ネットワーク管理ソフトウェア(NNM)からはアクセスできない	NNM からコマンドを実行する場合、ユーザ名がログインユーザと異なる場合があるようです。 CKID コマンドでユーザ名チェックを無効にするか、ユーザ名を NNM メーカーにお問合せください。

トラブル状態	推定原因と処置
Windows2000 から rsh を同時に大量送信すると、画面上にウィンドウが残る	rsh がタイムアウトを検出できないためにこのような現象が起こっているようです。 別売の ISA 製リモートシェル(irsh)ではタイムアウト検出が可能なので、このような症状は起こりません。irsh は Windows 95 / 98 / Vista / 2008 / 7 にも対応しています。必要な場合はお問合せください。詳細は http://www.isa-j.co.jp/product/softwares/others/IRSH/ を参照。
工場出荷時のユーザ名(DN1500)、パスワード(DN1500)を入力してもログインできない	ブラウザ側で大文字を小文字に自動変換するようになっていないか、ご確認ください。
ブラウザから http://xxx.xxx.xxx.xxx でアクセスした時に真白な画面が表示されアクセスできない	Windows サーバ系の PC などセキュリティ設定によりアクセスできない場合があります。その場合、http://xxx.xxx.xxx.xxx/cgi-bin/index.php でアクセスし、信頼済みサイトのゾーンに追加を行うことでアクセスできるようになります。

付録 B: 事前に必要なネットワーク関連情報

こんなとき	すること	必要項目	有線	無線	注意
ネットワークに接続する	IP アドレスの登録(※1)	IPv4 アドレス	○	○	
		IPv4 サブネットマスク	○	○	
		IPv6 アドレス	○	○	グローバル IPv6 アドレス　または ユニークローカルアドレス
		IPv4 ゲートウェイアドレス	△	△	
		IPv6 ゲートウェイアドレス	△	△	
無線 LAN を使用する	無線 LAN アクセスポイントの登録	アクティベーションキー	―	○	製品に同梱されているアクティベーションキー用紙と本体側面に貼付されているシールを確認ください。
		SSID	―	○	
		暗号化モード	―	○	
		暗号強度	―	○	WEP 利用の場合
		指定方法	―	○	WEP 利用の場合
		WEP キー	―	○	WEP 利用の場合
		WPA 共有キー	―	○	WPA/WPA2-PSK(TKIP/AES)利用の場合

※1 本製品は IPｖ4 と IPｖ6 のデュアルスタックのため、環境に合わせてネットワーク情報を登録してください。

こんなとき	すること	必要項目	必要性	注意
ホスト名を使用して設定する	DNS サーバの登録	プライマリ DNS サーバドレス	○	DNS サーバは IPv4･IPv6　どちらも使用することができます。
		セカンダリ DNS サーバドレス	○	
NTP サーバと同期させる	NTP サーバの登録	NTP サーバドレス	○	
メールを送信する	電子メール設定	SMTP サーバドレス	○	
		ポート番号	○	
		認証ユーザ名	△	認証方式により必要
		認証パスワード	△	認証方式により必要
		POP3 サーバドレス	△	POP before SMTP 利用の場合
		POP3 ポート番号	△	POP before SMTP 利用の場合

付録 C: rsh 通信における使用ポートについて

rsh 通信を Firewall で許可する場合は、以下のポートの利用を許可します。

コマンド送信元から警告灯へ片方向の許可：514/tcp
コマンド送信元と警告灯の両方向の許可：1020/tcp～1023/tcp

なお、1000 番台のポートについては、初めに 1023/tcp を利用しようとして、利用中の場合は 1022、1021…と空いてるポートを OS が自動で選択します。そのため、通信量の多い環境においては、1020 番よりも番号の若いポートを許可する必要があります。

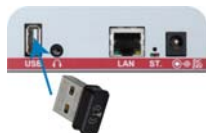
ポリシーの関係上、多数のポート許可が出来ない場合、snmp コマンド（snmpset）を用いてください。ただし、snmp コマンドは UDP 通信のため TCP 通信の信頼性が保たれませんので、ご注意ください。

※　snmp コマンドの許可ポートは 161/udp　となります。
※　rsh コマンドを UDP で使用することは出来ません。

付録 D: 別売の無線 LAN キット(DN-1500GL-WK)を設置/設定するには

無線 LAN キット(DN-1500GL-WK)は、DN-1500GL-N シリーズに後付けし、無線 LAN 対応にする製品です。
→下記手順にて「警子ちゃん 4G 本体設定ツール」より「アクティベーションキー」および「無線 LAN IP アドレス」「無線 LAN アクセス」情報の設定、および　無線 LAN □有効 にチェックし設定いただくことで、無線 LAN 対応環境下にてご使用いただけます。

手順

1 無線 LAN アダプタを警子ちゃん 4G 本体(背面)へ差し込む

※差込方向に注意してください。
※弊社製品以外の市販品の無線 LAN モジュールなどを差し込まれても、ご使用いただけません。

2 警子ちゃん 4G 本体設定ツールにて登録
警子ちゃん 4G 本体設定ツールへログイン
[基本情報] LAN 設定　→　無線 LAN アクセス欄 □有効 チェック および 情報入力
（※無線 LAN IP アドレス 含む）
【アクティベーションキー】欄へ、無線 LAN キットに同梱の簡易取扱説明書に記載されているアクティベーションキーを入力
画面下の「設定」ボタンをクリックし、設定値に反映させます。

3 無線 LAN 確認
①　無線 LAN の設定が有効になると、アダプタ本体の LED(青)が点滅します。
②　無線 LAN に設定した IP アドレスで web 設定ツールが表示できるか確認ください。

付録 E: サポート/サービスについて

ご購入前でも、電話や電子メールによるお問い合わせについては回答を差し上げるサポートを行っております。

ご購入後は、修理依頼や異常解析などのお問い合わせもありユーザ登録済みの確認をさせていただいています。ご購入後は、できるだけ早い時期に「ユーザ登録」を済ませてください。

E-1 ユーザ登録について

本製品には「お客様登録 FAX カード」を同梱しております。

お客様登録 FAX カードへ必要事項をご記入いただき、ただちに返信していただくか、弊社ホームページよりユーザ登録を行ってください。

ユーザ登録 URL： http://www.isa-j.co.jp/support/user/

※ ユーザ登録をお済ませいただかないと、製品ダウンロードサイトへアクセス出来ません。ご注意ください。

[注 意]
製品保証期間は、ユーザ登録後 1 年間(センドバック方式対応)となります。
※ユーザ登録されていないお客様については保証期間内であってもサービスが受けられない場合があります。ご注意ください。

E-2 修理を依頼されるとき

異常がある場合は、使用をやめてお買い上げの販売店へ修理をお申しつけください。

[危 険]
お客様自身での修理は危険ですので、絶対に行わないでください。

■保証期間中:
お買い上げの販売店に修理をお申しつけください。「保証規定」に従って無償で修理致します。

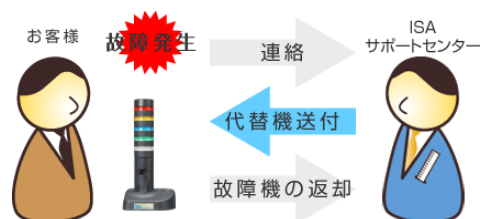
【ご連絡いただきたい内容】
品名：(警子ちゃん 4G)
モデル名：(DN-1500GL-xxxxx　xxxxx の部分が重要です)
お買い上げ日：お買い上げの販売店名
故障の状態(できるだけ具体的に)：

■保証期間後：
お買い上げの販売店にご相談ください。不具合箇所を確認し、お見積もり確認の後、有償にて修理いたします。

※ 本装置の設計寿命は約 5 年です。
※ 別途保守サービス(有償)メニューを用意しております。ぜひご検討ください。

E-3 保守サービス(有償)について

● 安心してご利用いただくために ●

本製品(警子ちゃん 4G シリーズ)では、ご購入後、お客様に安心して長期にご利用いただくための保守サービスをご用意しております。特に５年パック保守は、単年契約を繰り返す手間が省けるうえに費用も大変お得となっております。

代替機の先出し修理方式：

保守サービスに加入頂きますと、サービス期間中の故障時には代替機との交換をさせていただきます。お客様からご連絡をいただき、故障と判断した場合、先に代替機を発送しますので時間ロスも短縮できます。修理作業費や部品代なども発生しないため、スポット修理に比べてお得なサービスになっています。

保守サービスメニューご案内 URL：
http://www.isa-j.co.jp/keiko-10th/products/3g/support.html

安心の「先出しセンドバック」保守サービス

万が一、本製品(警子ちゃん 4G シリーズ)が故障した場合、「保守サービス証(正式版)」をお手元に置き、弊社カスタマーサポートセンターにご連絡ください。弊社サービス担当が故障と判断した場合、代替機をお客様宛に送付いたします。(就業時間内受付で当日発送となります。)

代替機到着後、お客様にて交換いただき、故障機をご返送いただきます。代替機は修理完了後本体が戻るまでご利用いただけます。

※ 単年度保守は、購入後１年目または２年目にてご契約となります。
※ ５年パック保守は製品本体と同時購入が前提となります。
※ 保守サービスご希望の場合は、製品をご購入いただいた販売店へお問い合わせください。
※ 本サービスを日本国内の離島や山岳地等交通手段が限定される地域、あるいは海外でのご利用をお考えの際は、事前にお問い合わせください。

本製品(警子ちゃん 4G シリーズ) 保守サービス契約料金/概要 (2013 年 1 月現在)

内　容	標準小売価格(税別)/台		説　明
	初年度	次年度以降	
５年パック保守	(５年間まとめて) 30,000 円	―	５年パック保守： ５年間を１パックにし、保守料金も単年度保守よりも割安です。
単年度保守	11,400 円	11,400 円	単年度保守： １年毎の保守サービスです。 次年度以降も同額保守料金でサポートいたします。

付録 F: 保証規定

1　取扱説明書に従った正常な使用状態で保証期間内に故障した場合には、引取にて無償修理させていただきます。
この場合お客様が、ご使用システムから故障機器を「切り離し」下記窓口へお送りください。

2　修理品の輸送料金及び諸掛かりはお客様の負担となります。
輸送される場合は輸送中の破損がないように適切な梱包を行ってください。

3　保証期間内でも次のような場合は有料修理になります。
(イ)取扱上の不注意による故障及び損傷
(ロ)不当な修理や改造による故障及び損傷
(ハ)火災、地震、水害、雷、その他の天災地変及び異常電圧による故障及び損傷
(ニ)お買い上げ後の輸送、移動時のお取扱いが不適当なために生じた故障及び損傷
(ホ)分解、もしくは分解したと思われる形跡(傷跡･半田跡等)が確認された場合
(へ)ユーザ登録されていないお客様の場合
(ト)本製品に接続している当社指定機器以外の機器の故障によって生じた故障
(チ)消耗部品及び付属品の交換

その他
・本装置使用中において、本装置及び接続されるシステムに万一不具合や故障が発生しても原因の如何を問わずその結果については責任を負いかねます。
・アフターサービスについてご不明な点は、お買い上げの販売店または下記までご連絡ください。

株式会社アイエスエイ　国内営業部
〒160-0022 東京都新宿区新宿 6-24-16
お電話によるお問い合せは　03-3208-1563
FAX によるお問い合せは　03-3208-1335
E-mail によるお問い合せは　info@isa-j.co.jp

付録 G: 問い合わせ票(E-mail･FAX)〔製品：DN-1500GL〕

株式会社アイエスエイ カスタマーサポートグループ宛

TEL：03-3208-1243　FAX：03-3208-1335

▼下記、ご記入の上、E-mail(info@isa-j.co.jp)　または　FAX(03-3208-1335)　にてご依頼ください。

※ は、記入必須項目となります。

ご依頼日		年	月	日
お客様情報	フリガナ		TEL ※	
	名　前 ※		FAX ※	
			E-mail	
	フリガナ			
	会社名 ※			
	フリガナ			
	部署名※			
	フリガナ			
	住　所 ※			

製品・その他情報		
	製品名	
	本体シリアル番号	
	ユーティリティソフトまたはファームウェアバージョン	

使用マシン情報		
	マシン名	
	ご使用の OS 名	

問い合わせへのご望回答方法は？ (該当 □ に、チェックください。)

□　FAX による回答　　□　TEL による回答　　□　E-mail による回答

お問い合わせ内容の詳細(できるだけ、詳しく記入してください)

返送先：

〒160-0022 東京都新宿区新宿 6-24-12 新宿 6 丁目ビル

株式会社アイエスエイ　カスタマーサポート宛

E-mail：info@isa-j.co.jp　TEL：03-3208-1243　FAX：03-3208-1335

株式会社アイエスエイの個人情報保護について　http://www.isa-j.co.jp/keiko-10th/privacy.html

■弊社使用欄

付録 H: イベントログ一覧

2012 年 9 月 3 日改定

イベントログとして記録される項目は、以下をご参照ください。

ログメッセージ	説明
boot	起動完了
reboot (initialize)	設定初期化による再起動完了
reboot (FW update)	ファームウェアアップデートによる再起動完了
対象 nn ($$$) 警報 On 対象 nn ($$$) 警報 Off	ネットワーク監視検出 nn：監視設定の登録番号 $$$：監視アドレス
トラップ n ($$$) 受信	SNMP トラップ受信 n：監視受信トラップの登録番号 $$$：監視受信トラップの説明
TCP xxxx ######## addr	TCP ソケット通信コマンド受信 xxxx：コマンド名 ########：コマンド引数 addr：送信元 IP アドレス コマンドエラー時は xxxx は以下の内容 xxxx="ER01"：無効なコマンド xxxx="ER02"：行末コードが異なる xxxx="ER03"：コマンド引数が間違っている xxxx="ER04"：コマンド実行失敗
RSH xxxx ######## addr	RSH コマンド受信 xxxx：コマンド名 ########：コマンド引数 addr：送信元 IP アドレス
SNMP xxxx ########	SNMP コマンド受信 xxxx：コマンド名 ########：コマンド引数
スイッチによるブザー/音声解除	アラームストップボタンによるブザー/音声解除
スイッチによるアラーム解除	アラームストップボタンによるアラーム解除
ツールによるアラーム解除	WEB 設定ツールの全アラーム解除実行
メール送信失敗	メール送信エラー
コマンド実行失敗	コマンド実行エラー
NTP 同期失敗	NTP サーバへの時刻同期に失敗した

付録 I: SNMP MIB (OID) 一覧(DN-1500GL)

2013 年 1 月 21 日改定

x=.iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).isa(1333).product(1).data-net(2).dn1500(6)

OID	ObjectName	SYNTAX	MAX-ACCESS	DESCRIPTION
x.1	ident	-	-	
x.1.1.0	identUnitID	OCTET STRING (SIZE (4))	read-only	ISA DN シリーズの装置識別子
x.1.2.0	identVersion	OCTET STRING (SIZE (9))	read-only	F/W Version
x.1.3.0	identModelName	OCTET STRING (SIZE (0..30))	read-only	モデル名
x.1.4.0	identLampId	OCTET STRING (SIZE(1))	read-only	ランプコード 5: 5L 3: 3L
x.1.5.0	identlSerialNumber	OCTET STRING (SIZE(10))	read-only	シリアル番号
x.1.6.0	identProductDate	OCTET STRING (SIZE(4))	read-only	製造年月 YYMM
x.1.7.0	identContractNumber	OCTET STRING (SIZE(6))	read-only	保守契約番号
x.1.8.0	identContractDate	OCTET STRING (SIZE(10))	read-only	保守契約期限
x.1.9.0	identDescription	OCTET STRING or Hex- STRING	read-only	機器説明
x.2	config	-	-	
x.2.1	self	-	-	
x.2.1.10	selfEth0MacAddr	OCTET STRING	read-only	有線 LAN MAC アドレス
x.2.1.2.0	selfEth0IPv4Addr	IpAddress	read-only	有線 LAN IPv4 アドレス
x.2.1.3.0	selfEth0IPv4SubnetMask	IpAddress	read-only	有線 LAN IPv4 サブネットマスク
x.2.1.4.0	selfEth0IPv4GatewayAddr	IpAddress	read-only	有線 LAN IPv4 デフォルトゲートウェイアドレス
x.2.1.5.0	selfEth0IPv4GatewayMetric	Integer32	read-only	有線 LAN IPv4 デフォルトゲートウェイメトリック値
x.2.1.6.0	selfEth0IPv6LinkLocalAddr	Ipv6Address	read-only	有線 LAN IPv6 リンクローカルアドレス
x.2.1.7.0	selfEth0IPv6Addr	Ipv6Address	read-only	有線 LAN IPv6 アドレス
x.2.1.8.0	selfEth0IPv6PrefixLength	Integer32	read-only	有線 LAN IPv6 アドレス プレフィックス長
x.2.1.9.0	selfEth0IPv6GatewayAddr	Ipv6Address	read-only	有線 LAN IPv6 デフォルトゲートウェイアドレス
x.2.1.10.0	selfEth0IPv6GatewayMetric	Integer32	read-only	有線 LAN IPv6 デフォルトゲートウェイメトリック値
x.2.1.11.0	selfEth0Speed	OCTET STRING	read-only	有線 LAN 接続スピード
x.2.1.12.0	selfEth1MacAddr	OCTET STRING	read-only	有線 LAN MAC アドレス
x.2.1.13.0	selfEth1IPv4Addr	IpAddress	read-only	Eth1 IPv4 アドレス
x.2.1.14.0	selfEth1IPv4SubnetMask	IpAddress	read-only	Eth1 IPv4 サブネットマスク
x.2.1.15.0	selfEth1IPv4GatewayAddr	IpAddress	read-only	Eth1 IPv4 デフォルトゲートウェイアドレス
x.2.1.16.0	selfEth1IPv4GatewayMetric	Integer32	read-only	Eth1 IPv4 デフォルトゲートウェイメトリック値

OID	ObjectName	SYNTAX	MAX-ACCESS	DESCRIPTION
x.2.1.17.0	selfEth1IPv6LinkLocalAddr	Ipv6Address	read-only	Eth1 IPv6 リンクローカルアドレス
x.2.1.18.0	selfEth1IPv6Addr	Ipv6Address	read-only	Eth1 IPv6 アドレス
x.2.1.19.0	selfEth1IPv6PrefixLength	Integer32	read-only	Eth1 IPv6 アドレス　プレフィックス長
x.2.1.20.0	selfEth1IPv6GatewayAddr	Ipv6Address	read-only	Eth1 IPv6 デフォルトゲートウェイアドレス
x.2.1.21.0	selfEth1IPv6GatewayMetric	Integer32	read-only	Eth1 IPv6 デフォルトゲートウェイメトリック値
x.2.1.22.0	selfEth1Speed	OCTET STRING	read-only	Eth1 接続スピード
x.2.1.23.0	selfWlan0MacAddr	OCTET STRING	read-only	無線 LAN MAC アドレス
x.2.1.24.0	selfWlan0IPv4Addr	IpAddress	read-only	無線 LAN IPv4 アドレス
x.2.1.25.0	selfWlan0IPv4SubnetMask	IpAddress	read-only	無線 LAN IPv4 サブネットマスク
x.2.1.26.0	selfWlan0IPv4GatewayAddr	IpAddress	read-only	無線 LAN IPv4 デフォルトゲートウェイアドレス
x.2.1.27.0	selfWlan0IPv4GatewayMetri c	Integer32	read-only	無線 LAN IPv4 デフォルトゲートウェイメトリック値
x.2.1.28.0	selfWlan0IPv6LinkLocalAddr	Ipv6Address	read-only	無線 LAN IPv6 リンクローカルアドレス
x.2.1.29.0	selfWlan0IPv6Addr	Ipv6Address	read-only	無線 LAN IPv6 アドレス
x.2.1.30.0	selfWlan0IPv6PrefixLength	Integer32	read-only	無線 LAN IPv6 アドレス　プレフィックス長
x.2.1.31.0	selfWlan0IPv6GatewayAddr	Ipv6Address	read-only	無線 LAN IPv6 デフォルトゲートウェイアドレス
x.2.1.32.0	selfWlan0IPv6GatewayMetri c	Integer32	read-only	無線 LAN IPv6 デフォルトゲートウェイメトリック値
x.2.1.33.0	selfWlan0Speed	OCTET STRING	read-only	無線 LAN 接続スピード
x.2.1.34.0	selfDnsPrimary	OCTET STRING	read-only	プライマリ DNS サーバアドレス
x.2.1.35.0	selfDnsSecondary	OCTET STRING	read-only	セカンダリ DNS サーバアドレス
x.3	ctrl	-	-	
x.3.1.0	ctrlACOP	OCTET STRING (SIZE (8))	read-write	ランプ/ブザー出力状態制御 1：点灯 （ブザー：連続音） 2：消灯 （ブザー：停止） 3：点滅 （ブザー：断続音） 4：高速点滅 X：状態保持

OID	ObjectName	SYNTAX	MAX-ACCESS	DESCRIPTION
x.3.2.0	ctrlSPOP	OCTET STRING (SIZE (8))	read-write	音声出力状態制御 【第１オクテット】 出力： ０：停止 １：再生 【第２、３オクテット】 再生する音声の番号：（01～20） 【第４オクテット リピート０：連続 １：回数指定 【第５、６オクテット】 リピート回数：（01-99） 【第７オクテット】 音声再生前のブザー出力： ０：なし　１：あり 【第８オクテット】 Reserved
x.3.3.0	ctrlALOF	Integer32 {ALOF(1)}	read-write	全アラーム停止
x.3.4.0	ctrlNodeMonior	OCTET STRING (SIZE (20))	read-write	ネットワーク監視 有効/無効設定： E=有効 D=無効 X=状態保持 設定状態、監視状態の 読み出し： E=有効(正常) F=有効(警告) D=無効
x.3.5.0	ctrlTrapMonitor	OCTET STRING (SIZE (40))	read-write	トラップ監視有効/無効設定： E=有効 D=無効 X=状態保持 設定状態の読み出し： E=有効 D=無効

x.3.8.1.1.0	ctrlRly1	INTEGER {
		on(1),
		off(2),
		blink(3),
		quickBlink(4)
		}
			read-write	Relay1(赤ランプ)出力制御
				１：点灯
				２：消灯
				３：点滅　４：高速点滅

x.3.8.1.2.0	ctrlRly2	INTEGER {
		on(1),
		off(2),
		blink(3),
		quickBlink(4)
		}
			read-write	Relay2(黄ランプ)出力制御
				１：点灯
				２：消灯
				３：点滅　４：高速点滅

x.3.8.1.3.0	ctrlRly3	INTEGER {
		on(1),
		off(2),
		blink(3),
		quickBlink(4)
		}
			read-write	Relay3(緑ランプ)出力制御
				１：点灯
				２：消灯
				３：点滅　４：高速点滅

OID	ObjectName	SYNTAX	MAX-ACCESS	DESCRIPTION

x.3.8.1.4.0	ctrlRly4	INTEGER {
		on(1),
		off(2),
		Blink(3)
		}
			read-write	Relay4(ブザー連続音
				(PPP・・・))出力制御
				1：ブザー音鳴動
				2：ブザー音停止
				3：ブザー断続鳴動

x.3.8.1.5.0	ctrlRly5	INTEGER {
		on(1),
		off(2),
		Blink(3)
		}
			read-write	Relay5(ブザー断続音
				(P-P-P-・・・))出力制御
				1：ブザー音鳴動
				2：ブザー音停止
				3：ブザー断続鳴動

x.3.8.1.6.0	ctrlRly6	INTEGER {
		on(1),
		off(2),
		blink(3),
		quickBlink(4)
		}
			read-write	Relay6(青ランプ)出力制御
				1：点灯
				2：消灯
				3：点滅
				4：高速点滅

x.3.8.1.7.0	ctrlRly7	INTEGER {
		on(1),
		off(2),
		blink(3),
		quickBlink(4)
		}
			read-write	Relay7(白ランプ)出力制御
				1：点灯
				2：消灯
				3：点滅
				4：高速点滅

x.3.8.1.8.0	ctrlRly8	INTEGER {
		on(1),
		off(2),
		blink(3),
		quickBlink(4)
		}
			read-write	Relay8 出力制御
				※Reserved

※ 従来機種(DN-1300GL、DN-1000R シリーズ、DN-1000S)との互換性

以下の ObjectName の Object は DN-1300GL、DN-1000R シリーズ、DN-1000S で定義されている OID にてアクセス可能です。

identUnitID(ctrlUnitID)、identVersion(ctrlVersion)、identModelName(ctrlModelname)、identLampId(ctrlLampId)、identSerialNumber(ctrlSerialNumber)、identProductDate(ctrlProductDate)、selfEth0MacAddr(ctrlEthAddr)、selfEth0IPv4Addr(ctrlIPAddr)、selfEth0IPv4GatewayAddr(ctrlGatewayAddr)、selfEth0IPv4SubnetMask(ctrlSubnetMask)、ctrlACOP、ctrlALOF、ctrlRly1～ctrlRly8

付録 J: SNMP トラップ一覧

enterprise	generic-trap	specific trap	内容
.1.3.6.1.4.1.1333.1.2.6.4.1	6	1	ネットワークモニタ 1 異常
.1.3.6.1.4.1.1333.1.2.6.4.1	6	2	ネットワークモニタ 1 回復
.1.3.6.1.4.1.1333.1.2.6.4.1	6	3	ネットワークモニタ 2 異常
.1.3.6.1.4.1.1333.1.2.6.4.1	6	4	ネットワークモニタ 2 回復
.1.3.6.1.4.1.1333.1.2.6.4.1	6	5	ネットワークモニタ 3 異常
.1.3.6.1.4.1.1333.1.2.6.4.1	6	6	ネットワークモニタ 3 回復
.1.3.6.1.4.1.1333.1.2.6.4.1	6	7	ネットワークモニタ 4 異常
.1.3.6.1.4.1.1333.1.2.6.4.1	6	8	ネットワークモニタ 4 回復
.1.3.6.1.4.1.1333.1.2.6.4.1	6	9	ネットワークモニタ 5 異常
.1.3.6.1.4.1.1333.1.2.6.4.1	6	10	ネットワークモニタ 5 回復
.1.3.6.1.4.1.1333.1.2.6.4.1	6	11	ネットワークモニタ 6 異常
.1.3.6.1.4.1.1333.1.2.6.4.1	6	12	ネットワークモニタ 6 回復
.1.3.6.1.4.1.1333.1.2.6.4.1	6	13	ネットワークモニタ 7 異常
.1.3.6.1.4.1.1333.1.2.6.4.1	6	14	ネットワークモニタ 7 回復
.1.3.6.1.4.1.1333.1.2.6.4.1	6	15	ネットワークモニタ 8 異常
.1.3.6.1.4.1.1333.1.2.6.4.1	6	16	ネットワークモニタ 8 回復
.1.3.6.1.4.1.1333.1.2.6.4.1	6	17	ネットワークモニタ 9 異常
.1.3.6.1.4.1.1333.1.2.6.4.1	6	18	ネットワークモニタ 9 回復
.1.3.6.1.4.1.1333.1.2.6.4.1	6	19	ネットワークモニタ 10 異常
.1.3.6.1.4.1.1333.1.2.6.4.1	6	20	ネットワークモニタ 10 回復
.1.3.6.1.4.1.1333.1.2.6.4.1	6	21	ネットワークモニタ 11 異常
.1.3.6.1.4.1.1333.1.2.6.4.1	6	22	ネットワークモニタ 11 回復
.1.3.6.1.4.1.1333.1.2.6.4.1	6	23	ネットワークモニタ 12 異常
.1.3.6.1.4.1.1333.1.2.6.4.1	6	24	ネットワークモニタ 12 回復
.1.3.6.1.4.1.1333.1.2.6.4.1	6	25	ネットワークモニタ 13 異常
.1.3.6.1.4.1.1333.1.2.6.4.1	6	26	ネットワークモニタ 13 回復
.1.3.6.1.4.1.1333.1.2.6.4.1	6	27	ネットワークモニタ 14 異常
.1.3.6.1.4.1.1333.1.2.6.4.1	6	28	ネットワークモニタ 14 回復
.1.3.6.1.4.1.1333.1.2.6.4.1	6	29	ネットワークモニタ 15 異常
.1.3.6.1.4.1.1333.1.2.6.4.1	6	30	ネットワークモニタ 15 回復
.1.3.6.1.4.1.1333.1.2.6.4.1	6	31	ネットワークモニタ 16 異常
.1.3.6.1.4.1.1333.1.2.6.4.1	6	32	ネットワークモニタ 16 回復
.1.3.6.1.4.1.1333.1.2.6.4.1	6	33	ネットワークモニタ 17 異常
.1.3.6.1.4.1.1333.1.2.6.4.1	6	34	ネットワークモニタ 17 回復
.1.3.6.1.4.1.1333.1.2.6.4.1	6	35	ネットワークモニタ 18 異常
.1.3.6.1.4.1.1333.1.2.6.4.1	6	36	ネットワークモニタ 18 回復
.1.3.6.1.4.1.1333.1.2.6.4.1	6	37	ネットワークモニタ 19 異常
.1.3.6.1.4.1.1333.1.2.6.4.1	6	38	ネットワークモニタ 19 回復
.1.3.6.1.4.1.1333.1.2.6.4.1	6	39	ネットワークモニタ 20 異常
.1.3.6.1.4.1.1333.1.2.6.4.1	6	40	ネットワークモニタ 20 回復
.1.3.6.1.4.1.1333.1.2.6.4.2	6	1	SNMP トラップ 1 受信
.1.3.6.1.4.1.1333.1.2.6.4.2	6	2	SNMP トラップ 2 受信
.1.3.6.1.4.1.1333.1.2.6.4.2	6	3	SNMP トラップ 3 受信
.1.3.6.1.4.1.1333.1.2.6.4.2	6	4	SNMP トラップ 4 受信
.1.3.6.1.4.1.1333.1.2.6.4.2	6	5	SNMP トラップ 5 受信
.1.3.6.1.4.1.1333.1.2.6.4.2	6	6	SNMP トラップ 6 受信
.1.3.6.1.4.1.1333.1.2.6.4.2	6	7	SNMP トラップ 7 受信
.1.3.6.1.4.1.1333.1.2.6.4.2	6	8	SNMP トラップ 8 受信
.1.3.6.1.4.1.1333.1.2.6.4.2	6	9	SNMP トラップ 9 受信

enterprise	generic-trap	specific trap	内容
.1.3.6.1.4.1.1333.1.2.6.4.2	6	10	SNMP トラップ 10 受信
.1.3.6.1.4.1.1333.1.2.6.4.2	6	11	SNMP トラップ 11 受信
.1.3.6.1.4.1.1333.1.2.6.4.2	6	12	SNMP トラップ 12 受信
.1.3.6.1.4.1.1333.1.2.6.4.2	6	13	SNMP トラップ 13 受信
.1.3.6.1.4.1.1333.1.2.6.4.2	6	14	SNMP トラップ 14 受信
.1.3.6.1.4.1.1333.1.2.6.4.2	6	15	SNMP トラップ 15 受信
.1.3.6.1.4.1.1333.1.2.6.4.2	6	16	SNMP トラップ 16 受信
.1.3.6.1.4.1.1333.1.2.6.4.2	6	17	SNMP トラップ 17 受信
.1.3.6.1.4.1.1333.1.2.6.4.2	6	18	SNMP トラップ 18 受信
.1.3.6.1.4.1.1333.1.2.6.4.2	6	19	SNMP トラップ 19 受信
.1.3.6.1.4.1.1333.1.2.6.4.2	6	20	SNMP トラップ 20 受信
.1.3.6.1.4.1.1333.1.2.6.4.2	6	21	SNMP トラップ 21 受信
.1.3.6.1.4.1.1333.1.2.6.4.2	6	22	SNMP トラップ 22 受信
.1.3.6.1.4.1.1333.1.2.6.4.2	6	23	SNMP トラップ 23 受信
.1.3.6.1.4.1.1333.1.2.6.4.2	6	24	SNMP トラップ 24 受信
.1.3.6.1.4.1.1333.1.2.6.4.2	6	25	SNMP トラップ 25 受信
.1.3.6.1.4.1.1333.1.2.6.4.2	6	26	SNMP トラップ 26 受信
.1.3.6.1.4.1.1333.1.2.6.4.2	6	27	SNMP トラップ 27 受信
.1.3.6.1.4.1.1333.1.2.6.4.2	6	28	SNMP トラップ 28 受信
.1.3.6.1.4.1.1333.1.2.6.4.2	6	29	SNMP トラップ 29 受信
.1.3.6.1.4.1.1333.1.2.6.4.2	6	30	SNMP トラップ 30 受信
.1.3.6.1.4.1.1333.1.2.6.4.2	6	31	SNMP トラップ 31 受信
.1.3.6.1.4.1.1333.1.2.6.4.2	6	32	SNMP トラップ 32 受信
.1.3.6.1.4.1.1333.1.2.6.4.2	6	33	SNMP トラップ 33 受信
.1.3.6.1.4.1.1333.1.2.6.4.2	6	34	SNMP トラップ 34 受信
.1.3.6.1.4.1.1333.1.2.6.4.2	6	35	SNMP トラップ 35 受信
.1.3.6.1.4.1.1333.1.2.6.4.2	6	36	SNMP トラップ 36 受信
.1.3.6.1.4.1.1333.1.2.6.4.2	6	37	SNMP トラップ 37 受信
.1.3.6.1.4.1.1333.1.2.6.4.2	6	38	SNMP トラップ 38 受信
.1.3.6.1.4.1.1333.1.2.6.4.2	6	39	SNMP トラップ 39 受信
.1.3.6.1.4.1.1333.1.2.6.4.2	6	40	SNMP トラップ 40 受信
.1.3.6.1.4.1.1333.1.2.6.4.3	6	1	ALARM　STOP ボタン ON
.1.3.6.1.4.1.1333.1.2.6.4.3	6	2	ALARM　STOP ボタン OFF
.1.3.6.1.4.1.1333.1.2.6.4.3	6	3	コールドスタート　（※1）
.1.3.6.1.4.1.1333.1.2.6.4.3	6	4	内部温度異常　　（※2）

付録 K: 本体仕様

型式	DN-1500GL-★5L■◆	DN-1500GL-★5L■◆
外観	（イメージは DN-1500GL-★5LCB）	（イメージは DN-1500GL-★5LSW）
外形寸法(mm)	160W / 125D / 330H	160 / 125D / 270H
質量(g)	820	820
ランプ	赤、黄、青、緑、白	赤、黄、青、緑、白
ブザー	断続音(P-、P-、P-、…、約 35 回/分)・連続音(PPPP…、約 700 回/分) 3.3kHz/70～90dB	
MPU	ARM アーキテクチャ 32bit 1.2GHz	
オーディオ出力	1ch、3.5mmΦミニジャック、ヘッドフォン出力(ステレオ、16Ω、46mW)*2	
有線 LAN	ギガビットイーサ (10BASE-T、100BASE-TX、1000BASE-T のオートネゴシエーション)	
無線 LAN	WiFi 準拠、IEEE802.11 b/g/n セキュリティ：Open System、WEP(64/128bit)、WPA/WPA-2-PSK(TKIP/ASE)	
USB	USB 2.0 (WiFi モジュール専用)	
セキュリティ	(暗号) AES、DES、3DES (認証) SHA1、MD5	
IP ネットワーク	IPv4、IPv6 およびデュアルスタック	
ノード監視	最大 20 ノード(IPv4、IPv6 ノード、ホスト名合わせて)	
ノード監視方式	ICMP Echo Reply(ping)のポーリングによる(応答時間閾値指定可能)	
SNMP トラップ監視	最大 40 トラップ Specific-trap、generic-trap、 文字列を含む最大 5 個までの variable-bindings による判定(最大 OID 長 256 文字/文字列)	
対応 SNMP	SNMPv1、SNMPv2c、SNMPv3	
音声ファイル	MP3 型式、最大 20 ファイル登録可能	
警報・通知	最大 60 のアクションを登録可能(ノード監視:20 アクション、トラップ監視:40 アクション) 警告灯の色、点滅・点灯、ブザーの断続・連続、および組合せによる警報 登録されている音声ファイルの再生(繰り返し回数指定可能) 最大 5 箇所への E-mail 送信(携帯電話含む)(SMTP、SMTPAuth)、送信先はアクション毎に選択可能 最大 5 箇所への SNMP トラップ送信 異常時、復帰時に指定スクリプト(rsh、snmpset など)を IP アドレス、またはホスト	

	名で実行
コマンドによる制御	rsh、snmpset コマンドおよび TCP ソケット通信による警告灯･ブザー･音声ファイルの制御可能 (警告灯の色、点灯・点滅、ブザーの断続・連続音、音声ファイルの再生およびその組合わせ指定)
NNM との連携	HP Software(旧 OpenView)、JP1、Systemwalker、Senju、Tivoli、e-Care、NOSiDE、TELstaff、WebSAM、Ci-NetworkMonitor、CentreNET Swim シリーズ、SNMPc、A-AUTO、PNDDA、Net-ADM、ProactiveNet、ManageEngine OpManager、 CLUSTERPRO X、 NetCrunch、PISO、 CA eHealth、PATROLCLARICE、SystemAnswer、ManagementCore、NetKids シリーズ、SIGNAlert、ZABICOM/Zabbix、WhatsUp Gold などの管理ソフトウェア等のアクション記述により、警告灯の点灯、ブザーの鳴動および音声ファイルの再生が可能異常発見時、NNM に SNMP トラップによる通知可能 異常発見時、NNM に SNMP トラップによる通知可能
設定情報バックアップ	本体の設定内容をバックアップ、およびリストア可能
NTP クライアント機能	登録した Time Server(NTP サーバ)との時刻同期可能　タイムゾーン設定可能
イベント･ログ	異常の発生、復帰などをタイムスタンプと共に記録 自動メール送信機能(イベントログを添付ファイルとしてメール送信) 停電・瞬断でも記録された内容は消えない
コマンド実行機能	異常時・回復時に rsh、または snmpset コマンドの実行が可能
設定方式	Web ブラウザによる
ソフトウェア	Web 上よりファームウェア･アップデート可能
サポートプロトコル	ARP、HTTP、ICMP、RSH、NTP、SMTP、SNMP(v1 / v2c / v3)、SSH、TCP/IP、UDP
カレンダ/時計	コンデンサバックアップ
アラーム解除ボタン	有(ランプ・ブザーテストボタンを兼ねる) / 電源ランプを兼ねる
待機点灯	通常状態時、緑ランプ(3 灯モデル)または緑･青･白ランプの一つ(5 灯モデル)を点灯/点滅させ、監視中であることを明示的に表示することが可能
ステータス表示（LED）	Link/Activity、Speed(10Mbps/100Mbps/1Gbps)、WatchDog、Error
自己診断	WatchDog による監視　内蔵温度センサによる筐体内温度の異常判定
使用環境条件	温度：0～45℃　湿度：20%～85%RH (結露しないこと)　標高：3,000m 以下
電源 (AC アダプタ)	寸法(mm)：46W x 34D x 25H　(突起部、ケーブル含まず) 入力電圧：100 - 240VAC 50/60Hz　出力電圧： 24VDC 0.5A 質量：約 100g　　ケーブル長：約 1.6m

※型式 DN-1500GL-★●●■◆

★＝LAN タイプ	●●＝ランプ灯数	■＝レンズ色	◆＝ボディー色
A：無線 LAN 対応	5L： 5 灯タイプ	C：色付きレンズ	B：ダークグレー
N：無線 LAN 未対応	3L： 3 灯タイプ	S：透明レンズ	W：ライトグレー

付録 L: 14.150.0G 以前のファームウェアお使いの場合

バージョン：14.150.0G より以前のファームウェアで、SNMP トラップ監視をお使いの場合、generic または specific を空欄で設定した際、自動的に“0”が入力されます。

14.160.0G 以降のバージョンでは、空欄設定時は空欄になる様に仕様変更しています。

ファームウェアアップデート時またはリストア時、generic または specific の項目に“0”が設定されている場合は 空欄に上書きしてください。